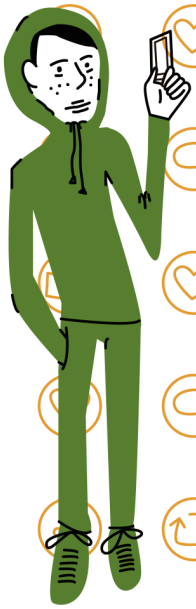
INFORME **2018**

¿DÓNDE ESTÁN MIS DATOS?

INVESTIGADORA: CAROLINA BOTERO

ASISTENTE DE INVESTIGACIÓN: DAVID MARTÍN ESPITIA



Fundación Karisma

Fundación
Karisma

Bogotá, Colombia
2018

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos. Más información sobre el tema: http://www.documentoaccesible.com/#que-es.

Fundación Karisma hace un especial reconocimiento a otros proyectos similares como *¿Quién defiende tus datos?* de R3D México, *¿Quién defiende tus datos?* de TEDIC Paraguay, *Quem defende seus dados?* de Internet LAB Brasil, *¿Quién defiende tus datos?* de Hiperderecho Perú, *¿Quién defiende tus datos?* de Derechos Digitales Chile, *¿Quién defiende tus datos?* de ADC Digital Argentina y, a otros fuera de la región como *¿Quién defiende tus datos?* de Eticas Foundation España, *Who has your back?* de la Electronic Frontier Foundation y *Ranking Digital Rights* del Open Technology Institute, que han servido como inspiración para este proyecto. Agradecemos también a las personas de las empresas evaluadas que se reunieron con nosotros y que han estado trabajando en mejorar los resultados de su evaluación.

Autora:
Carolina Botero

Investigación:
David Martín Espitia

Revisión:
Juan Diego Castañeda
Amalia Toledo

Coordinación editorial:
Diego Mora Bello

Diseño gráfico:
Daniela Moreno

Diagramación:
Rubén Urriago

Este informe está disponible bajo Licencia Creative Commons Reconocimiento compartir igual 4.0.

Usted puede remezclar, retocar y crear a partir de esta obra, incluso con fines comerciales, siempre y cuando le de crédito al autor y licencien nuevas creaciones bajo las mismas condiciones. Para ver una copia de esta licencia visite:
https://creativecommons.org/licenses/by-sa/4.0/deed.es_ES.

TABLA DE CONTENIDOS

Introducción **5**

Sobre el informe **9**

Principales hallazgos **11**

Los resultados comparados de 2018 . . . . . **25**

I. Transparencia 25

II. Intimidad 27

III. Libertad de expresión 28

IV. Seguridad digital 29

La evaluación de cada empresa **31**

Claro 31

Telefónica-Movistar 34

ETB 38

Directv 41

Tigo-UNE 45

Emcali 49

Telebucaramanga 51

Metodología **53**

INTRODUCCIÓN

El escándalo que conocimos en 2018 referido a los servicios que la empresa Cambridge Analytica ofrecía a campañas electorales en el mundo, a partir de los datos de millones de personas que tenían cuentas en Facebook, materializó el temor de muchos sobre los riesgos que entraña la acumulación de datos de las personas. A través de las bases de datos que Facebook le compartió, Cambridge Analytica podía desvelar las preferencias políticas de las personas y usarlas para manipular sus decisiones electorales. Las empresas que nos prestan servicios por internet guardan mucha información nuestra. La forma como la protegen, importa. Mientras más sepamos de esto, tendremos más información para tomar decisiones y comprender nuestra forma de vida con la tecnología incorporada.

Una simplificación sobre qué es internet sería decir que es un servicio flexible de comunicaciones para llevar datos de un dispositivo a otro sin importar la naturaleza de estos, de dónde y cómo se conectan, o del tipo o contenido de los datos. Para que esto suceda hay un sinnúmero de facilitadores que nos permiten enviar correos, montar una página o leer el periódico; son muchas las actividades. Quienes facilitan esto son los intermediarios de internet.[1]

Su rol es clave en la vida actual. Cuando conectan personas y permiten ofrecer y buscar información son habilitadores de derechos como la libertad de expresión; a la libre asociación; el acceso a la información, la cultura, la educación y la ciencia. Por eso es importante que su trabajo garantice la privacidad, una comunicación libre de violencia, en entornos de pluralidad y respeto. Así se afirmó en la declaración conjunta sobre la libertad de expresión e internet de 2011[2].

1 OECD. (2011). The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing. Recuperado en http://dx.doi.org/10.1787/9789264115644-en.

2 Declaración conjunta sobre libertad de expresión e Internet. 1 de junio de 2011, Considerando No. 4. Recuperado en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2.

Existen muchos intermediarios de internet y con muchas particularidades. La Organización para la Cooperación y el Desarrollo Económico (OCDE) los clasifica en seis tipos según el tipo de actividad o servicio que ofrecen en la red. Por cada uno de estos intermediarios, se debería analizar la forma como responden a las obligaciones de derechos humanos. Ahora bien, ¿Dónde están mis datos? es una investigación que se enfoca en la situación local de una de estas categorías, los proveedores de servicios de internet (PSI).

Los PSI son las empresas que ofrecen la conexión. ¿Cómo responden estas empresas que nos dan la conectividad a sus obligaciones en materia de derechos humanos? Diferentes dimensiones de esta preguntas son el eje del trabajo detrás de *¿Dónde están mis datos? 2018* y se presentan en un formato de guía para que los servicios de los PSI se puedan comparar no solo desde el punto de vista del mercado –mejores precios, mayor cobertura–, sino también desde el punto de vista del respeto y la promoción de derechos humanos. Esperamos que, además, en el proceso las personas puedan usar este informe para analizar y acercar sus intereses, tanto en la dimensión de consumo como la de ciudadanía, al momento de contratar a la empresa que les provee la conexión a la red.

LOS PSI EN COLOMBIA

Según cifras del Ministerio de las TIC[3], en Colombia hay aproximadamente 6.5 millones de accesos a internet fijo y 11 millones de accesos a internet móvil. En cuanto al número de PSI, hay tres que concentran el 72% del mercado fijo y tres que concentran el 92% del mercado móvil. Las empresas con mayor concentración de internet fijo y móvil respectivamente son: Telmex (Claro) con 36,9% fijo y 52,8% móvil; UNE-TiGO con 20,2% fijo y 12% móvil y Colombia Telecomunicaciones (Telefónica Movistar) con 15,2% fijo y 28,8% móvil. En cuanto a internet fijo, aparte de ETB y Edatel-TiGO –que tienen una participación del 10% y el 3% respectivamente–, existe otro número de empresas locales –por ejemplo, Telebucaramanga y Emcali– que sumadas tienen una participación del 14% del mercado.

3 Ministerio de las TIC. *Boletín Trimestral de las TIC*. Segundo Trimestre de 2018. Cifras tomadas de: Gráfico 16. "Accesos de internet fijo por proveedor" y Gráfico 30. "Accesos a internet móvil por demanda por proveedor". Disponible en: https://colombiatic.mintic.gov.co/679/articles-80413_archivo_pdf.pdf

	Marca comercial	PSI	Número de accesos	Share
Internet fijo 2T/2018	Claro	Telmex	2.423.948	36,95
	Une/TIGo	UNE	1.325.817	20,21
	Telefónica	Colombia telecomunicaciones	1.001.954	15,27
		ETB	657.023	10,02
		Edatel	201.220	3,07
		Restantes	949.888	14,48
		Satelital	10.597	0,16
		Total	6.559.850	
Internet por tecnología de acceso		cable	3'567.612	54,40%
		xDSL	1'892.656	28,90%
		Fibra Óptica	837.245	12,80%
		otras tecnologías	262.337	4,00%
Internet móvil 2T/2018	Claro	Comcel	5.871.496	52,84
	Telefónica	Colombia telecomunicaciones	3.202.980	28,83
	Tigo	Colombia móvil	1.335.067	12,02
		UNE	0	0,00
		Avantel	472.865	4,26
		ETB	228.886	2,06
		Total	11.111.294	

En 2017, se incluyó en la evaluación a Telebucaramanga y Emcali con el fin de revisar también los compromiso de empresas proveedoras más pequeñas. Se eligieron estas dos empresas porque aparecen en las listas de proveedores de internet de Colombia que prestan un servicio de calidad, con mayor velocidad y cobertura.

La información muestra que estas empresas poseen puede revelar con quién hablamos, por cuánto tiempo, cuándo y desde dónde. También podrían identificar qué equipos usamos, cuáles son nuestros hábitos de consumo –por ejemplo, a qué restaurantes vamos, cuándo y a dónde viajamos, y con qué frecuencia, si la hay– e incluso con quién nos encontramos –siempre que se pueda determinar, por ejemplo, los celulares que estuvieron en un mismo lugar a una misma hora y asumiendo que cargamos siempre este dispositivo–. Ellas tienen esta información que se conoce como los metadatos de nuestras comunicaciones, porque la guardan y usan para poder prestarnos el servicio. Las empresas comparten nuestros datos, pero ¿con quién? y ¿por qué?

Estas empresas también son la puerta de entrada para la interceptación de comunicaciones y la retención de datos personales sobre ubicación geográfica o historial de

comunicaciones. Estas actividades, que solo deberían ser solicitadas por la Fiscalía General de la Nación o los organismos de inteligencia, puede revelar también el contenido de lo que comunicamos a otras personas. Además, una vez se cruzan y analizan los metadatos a que hicimos mención antes, dejan al descubierto mucha información de nuestra vida privada.[4]

Los PSI deben conciliar importantes tensiones. De un lado, el sector de las telecomunicaciones está fuertemente regulado: requieren de permisos del Estado para operar en el correspondiente país. Deben registrarse y son vigilados y sancionados con base en un marco legal bastante complejo que les impone obligaciones y presiones para compartir información y bloquear contenidos Por otro lado, están obligados, como sucede en Colombia, por principios constitucionales como el de la inviolabilidad de las comunicaciones, que les impone el deber de proteger nuestra información de modo que la entrega de información o el bloqueo de contenidos de las personas que contratan sus servicios sea una excepción que esté sujeta a estándares de derechos humanos. Cuando tienen que cumplir con una orden legítima que limita este principio, ¿sabe usted cómo lo hacen?

No solo el Estado provoca esta tensión con los PSI. Estas empresas usan nuestros datos para mejorar sus servicios, conocernos mejor como clientes y hacer prospectivas sobre su negocio. Es decir, nuestros datos hacen parte de su negocio, los usan para fines comerciales y publicitarios, ¿sabe usted cómo lo hacen?

Finalmente, recordemos que los PSI son protagonistas en el mantenimiento de la neutralidad de la red, es decir, en la prohibición de que los intermediarios de internet interfieran en el uso que las personas hacen de la red, siempre que este sea un uso legal. En el caso de los PSI esta prohibición tiene sentido porque tienen una posición privilegiada como puerta de acceso a la red y por tanto sus decisiones pueden influir sobre las aplicaciones, contenidos o servicios a las que acceden las personas y sobre la información que publican, es decir son claves para el ejercicio de la libertad de expresión.

Asimismo, esta posición que les permite controlar los contenidos y servicios a los que accedemos es frecuentemente aprovechada por los Estados, por ejemplo, para bloquear contenidos de explotación sexual infantil, así también puede ser abusada por los gobiernos cuando obligan a los PSI a cortar la conexión de internet en medio de protestas o durante elecciones como ha sucedido en Venezuela o en países africanos.

Conocer la forma como estas empresas se comprometen a proteger nuestros derechos y comprender la forma como lo hacen puede ayudar a fortalecer esa capacidad.

4 Para ampliar la información sobre la vigilancia de las comunicaciones en Colombia, pueden consultarse los siguientes documentos: Cortés, C. (2014). Vigilancia de las comunicaciones en Colombia. Bogotá, Colombia: Dejusticia, 18; Rivera, J.C. y Rodríguez, K. (2015). Vigilancia de las comunicaciones por la autoridad y protección de los derechos humanos en Colombia. San Francisco, EEUU: Electronic Frontier Foundation; Castañeda, J.D. (2016). ¿Es legítima la retención de datos en Colombia?. Bogotá, Colombia: Fundación Karisma; Pérez, G. (2016). Hacking Team: malware para la vigilancia en América Latina. Santiago, Chile: Derechos Digitales.

SOBRE EL INFORME

El informe ¿Dónde están mis datos? es una evaluación que hace anualmente la Fundación Karisma sobre las políticas corporativas de estas empresas y los compromisos que adquieren sobre la protección de nuestros derechos. Desafortunadamente, este informe no tiene el alcance de evaluar la forma como tales empresas ponen en práctica su compromiso. En 2018, el informe se enfoca especialmente en la libertad de expresión y la intimidad; analiza el compromiso que tienen con la transparencia; si adoptan políticas de inclusión y si asumen de forma responsable la protección de nuestros datos y su seguridad.

El propósito central del informe es poner en evidencia las políticas corporativas de los principales PSI, la forma como las ajustan al marco legal tanto en lo local como en relación con los estándares internacionales, y la forma como promueven, fortalecen o, por el contrario, debilitan el disfrute de los derechos de las personas en este entorno tecnológico.

La evaluación nos permite también identificar buenas prácticas en el respeto de nuestros derechos en el entorno digital y resaltarlas. Esto va más allá de mirar si las políticas cumplen con las obligaciones legales para buscar que tengan un compromiso efectivo con desarrollarlas. Para 2018, podemos confirmar que los resultados del ejercicio dan cuenta de una transformación en el sector: hay más transparencia. Las empresas nos dan más información y esto a Karisma le permite identificar vacíos también en la forma como el Estado actúa frente a las empresas en la protección de nuestros derechos.

La evaluación usa como marco los estándares internacionales de derechos humanos descritos en documentos de organismos internacionales como las Naciones Unidas (ONU) y la Organización de Estados Americanos (OEA), e incluso iniciativas más amplias como la *Global Network Initiative* (GNI). De esta forma, se consideraron para esta evaluación documentos como la resolución de la Asamblea General de la ONU sobre el derecho a la privacidad en la era digital[5]; los documentos de la Relatoría para la Li-

5 Asamblea General de ONU. (2013, 20 de noviembre). *El derecho a la privacidad en la era digital*. A/C.3/68/L.45/Rev.1. Disponible en: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1&referer=http://proteccion-datos.mx/2013/12/esresolucin-de-las-naciones-unidas-sobre-el-derecho-la-privacidad-en-la-era-digitalenunited-nations-resolution-privacy-digital-age/&Lang=S. http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_28_L27.pd

bertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH)[6]; los principios del GNI[7] y los Principios necesarios y proporcionales[8].

Con este documento, Karisma presenta el cuarto informe. Este año no se agregaron nuevos criterios de evaluación, pero sí se ajustó la metodología en algunos puntos para hacerla más exigente. Algunos de los criterios en 2017 otorgaban el punto si se cumplía tan solo con alguno de los supuestos. Así, por ejemplo, en la política de género se consideraban 5 componentes y con el cumplimiento de alguno se otorgaba el punto. En 2018, en cambio, el punto completo solo se obtiene si se acumulan los cinco elementos. De lo contrario, el valor será proporcional a los hallazgos (p.ej. si la empresa en su política de género considera tres de los cinco tópicos, recibirá 0,6 puntos).

Como lo hicimos en 2017, seguimos indagando sobre la existencia explícita de lenguaje incluyente, pero la mantenemos como una bonificación puesto que tiene el propósito de educar e impulsar la discusión sobre la diversidad sexual y de género en el sector de las tecnologías. En Karisma creemos que las preocupaciones que nos llevan a hacer este informe las asume mejor una empresa con una cultura sensible a los temas de género. Esperamos que en el futuro este sea un elemento transversal a la evaluación, es decir, que la perspectiva de género se evalúe en cada uno de los criterios elegidos (los detalles de la metodología empleada se describe en un capítulo de este documento).

Es importante también hablar del alcance limitado del informe. Por una parte, insistimos en que sabemos que hay otros temas importantes en la relación con el ejercicio de los derechos humanos. Es el caso de la sostenibilidad, la responsabilidad social empresarial, el compromiso con el medio ambiente, entre otros. Debemos aclarar que los ejes temáticos y los criterios que se usan en ¿Dónde están mis datos? corresponden a los fines misionales de Karisma. Por este motivo, muchos otros temas, aunque importantes, quedarán por fuera. De otra parte, el informe evalúa los compromisos públicos de los PSI, no sus prácticas o la forma como implementan esos compromisos. Es posible que algunos PSI tengan buenas prácticas en estos temas, pero que no tengan políticas o compromisos públicos. También es posible que la forma de actuar de algunos PSI no estén alineadas con sus propios compromisos públicos. Debido a la metodología y objetivos del informe, no será posible derivar nada de esto de los resultados del informe y sabemos que es un trabajo que sigue pendiente.

---

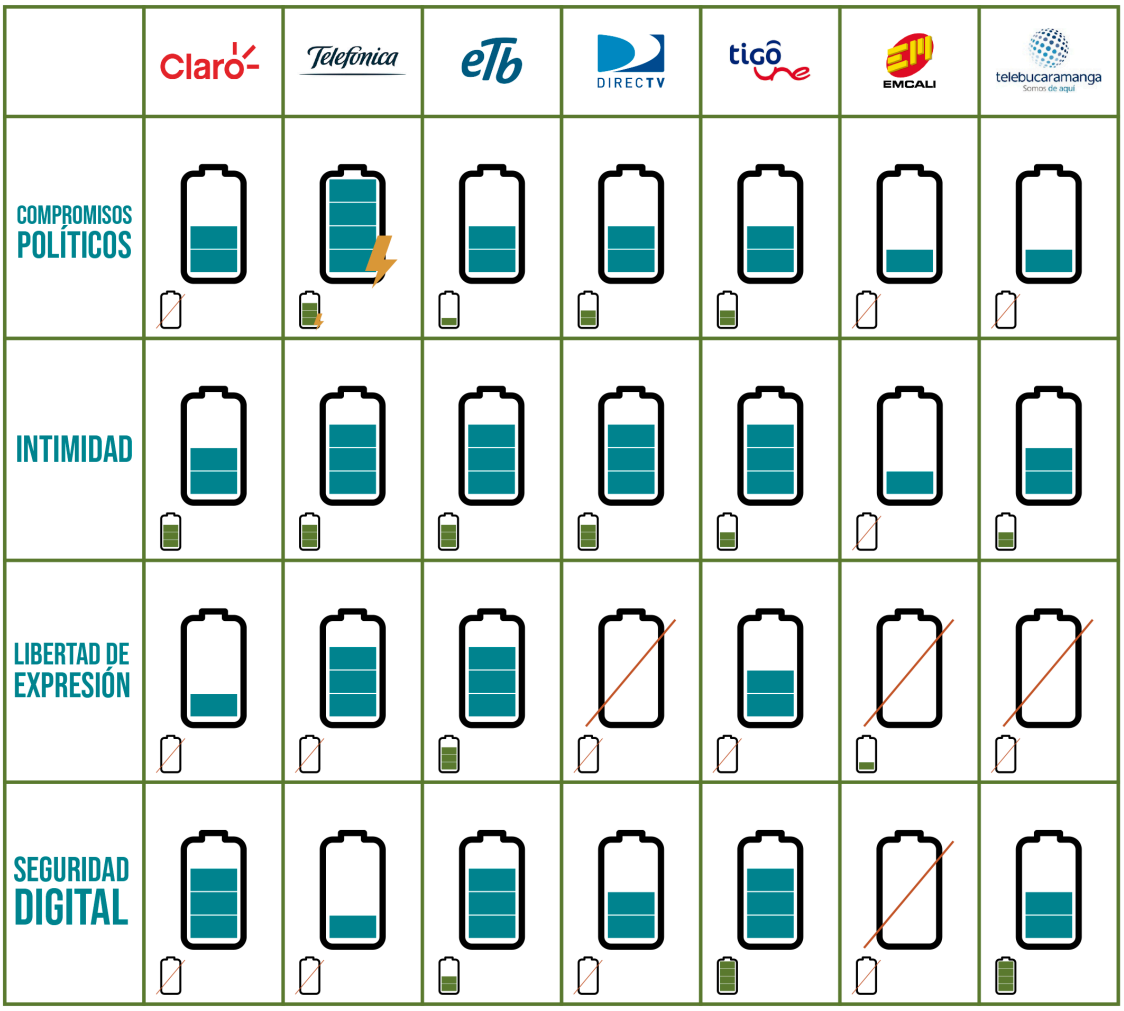
6 CIDH & RELE. (2013, 31 de diciembre). *Libertad de expresión e internet*. OEA/Ser.L/V/II. CIDH/RELE/INF.11/13. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf; *Declaración conjunta sobre libertad de expresión e internet de ONU OEA, OSCE y CADHP.* (2015). Disponible en http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849; CIDH & RELE. (2017, 15 de marzo). *Estándares para una Internet libre, abierta e incluyente*. OEA/Ser.L/V/IICIDH/RELE/INF.17/17. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf.

7 *GNI Principles on Freedom of Expression and Privacy*. (s.f.). Disponible en https://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy_0.pdf.

8 *Necesarios & proporcionados: principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones.* (2014, 10 de mayo). Disponible en: https://necessaryandproportionate.org/es/necesarios-proporcionados.

PRINCIPALES HALLAZGOS

TABLA GENERAL



CUMPLE TODOS LOS PARAMETROS

CUMPLE CASI SATISFACTORIAMENTE

CUMPLE PARCIALMENTE

2017

2018

PARCIALMENTE SEGURO

CUMPLE DE FORMA INSUFICIENTE

NO CUMPLE

BONIFICACIÓN POR LENGUAJE INCLUYENTE EN POLÍTICA DE GENERO

COMPLETAMENTE SEGURO

NO ES SEGURO

Las evaluaciones de ¿Dónde están mis datos? 2018 se llevaron a cabo durante dos períodos separados. Entre mayo y agosto de 2018, realizamos una evaluación preliminar que compartimos con las PSI evaluadas que se interesaron en conocer sus resultados. Después de esta primera experiencia, llevamos a cabo una evaluación final a mediados de octubre, que ajustamos tomando en cuenta los cambios recientes que las empresas nos mostraron o implementaron previo a este período. El proceso de revisión significó el cambio de algunos resultados iniciales.

En términos generales, todas las empresas mejoraron su puntaje en 2018. En los casos en que hubo algún deterioro, se debió sobre todo al hecho de que la evaluación se hizo más estricta y no porque se hubiera deteriorado la posición de la empresa.

Los **principales hallazgos** que encontramos en el 2018 fueron:

Informes de transparencia

- Más de la mitad de las empresas evaluadas publicaron información equivalente a un informe de transparencia, lo que consideramos como un avance importante. Mientras en 2017 solo una de las siete empresas evaluadas publicaba información que equivale a lo que internacionalmente se conoce como un informe de transparencia en el sector –aquellos donde se comunica al público qué información privada han solicitado y/o han accedido entidades gubernamentales y la forma como se comportan en relación con las solicitudes legales de bloqueos de contenidos–, en 2018 son cinco las empresas que entregan información local equivalente a un informe de transparencia tanto sobre solicitudes de datos personales como de bloqueos y filtrados de contenidos: ETB, Claro, Tigo-UNE y Telefónica-Movistar lo hacen en forma más precisa, mientras que Directv ofrece datos de solicitudes internacionales realizadas a su matriz.
- En los informes de ETB, Claro, Tigo-UNE y Telefónica podemos ver que nuestra información privada es solicitada y accedida por diferentes entidades gubernamentales, ya que la información que suministran indica qué autoridades la solicitan. Entre estas, se encuentran la Fiscalía General de la Nación, la Policía Nacional, el Ministerio de Defensa Nacional, la Dirección de Impuestos y Aduanas Nacionales, los municipios, el Instituto Colombiano de Bienestar Familiar, etcétera. ETB y Tigo-UNE muestran el número de peticiones de información admitidas y rechazadas en relación con el tipo de datos solicitados. Movistar da cifras más generales de requerimientos frente a las peticiones de datos personales. Claro no da cifras en materia de requerimientos de datos personales, pero es la que ofrece más información sobre los mecanismos de bloqueo legal de contenidos que se usan hoy en día. De una u otra forma, los informes que hacen explican los tipos de datos que se solicitan como datos biográficos, direcciones IP, datos geográficos, etcétera.

Políticas de protección de datos

- La tendencia a ofrecer mejor información que facilite a las personas conocer las políticas de protección de datos de estas empresas se mantiene en 2018, al punto que, con los criterios actuales, todas obtuvieron la máxima calificación. Por disposición legal, todas las empresas deben tener estas políticas. Hasta hace unos años esto se cumplía exclusivamente con la publicación de documentos difíciles de leer, con frecuencia copias de la ley, en formatos que no se podían navegar y a los que costaba trabajo llegar a través de sus sitios web. En 2018, todas las empresas evaluadas cuentan con documentos que no solo son públicos y claros, sino también están en formatos que permite navegarlos y reusarlos.
- La mayoría de las empresas evaluadas ofrecen la información sobre cómo protegen nuestra intimidad a un solo click de la página principal, en documentos para descargar. ETB y Emcali deben trabajar en facilitar el acceso a estos documentos, pues se encuentran a más de dos pasos de ser descubiertos por las personas desde la página principal. Vale la pena destacar el esfuerzo de Telefónica-Movistar por ir más allá de lo exigido legalmente y construir un micro sitio más amigable que permite conocer directamente y en forma sencilla las políticas de la empresa en este sentido. ETB y Tigo-UNE han centralizado en un sitio la información, lo que también es una forma más intuitiva de conocer las políticas de las empresas.

Solicitud de nuestra información por parte de autoridades

- En 2017, evaluamos positivamente el hecho de que las empresas declararan su compromiso legal de contarle a las personas cuando terceros habían solicitado su información, siempre que esa persona lo pidiera. En 2018, se hizo más estricto el criterio en la medida en que lo que se evalúa es el compromiso de las empresas en informar *siempre* que un tercero, incluido el Estado, solicita información personal de alguien. Aunque esta no es una obligación legal expresa en Colombia, sí es un estándar de derecho internacional que debería implementarse. Si bien este compromiso obliga a los Estados –que son los que deben respetar los derechos de defensa y debido proceso–, es el apoyo de estas empresas el que garantiza su efectivo ejercicio.[9] Ninguna de las empresas evaluadas cumple con este compromiso. A pesar de lo anterior, se debe reconocer un compromiso que adquiere Directv con las personas que usan sus servicios cuando afirma en su política de privacidad que *"en la mayoría de los casos en que la información se provee en respuesta a un requerimiento legal, nosotros le proveeremos notificación previa de dicho requerimiento u orden de modo que usted pueda impugnarla en un procedimiento en corte"*. Si bien no se puede decir que esta afirmación voluntaria

9 *Principios necesarios y proporcionales*, *op. cit.* (nota 6).

cumple con el requisito, es sin duda un compromiso que va en el sentido de lo que busca esta evaluación y así fue reconocida.

- En 2018, también hicimos más estricto el criterio sobre si las empresas informan acerca de su obligación de conservar nuestros datos y las razones para responder a requerimientos de información.[10] En general, las empresas informan que recogen datos y mencionan que cumplirán con las obligaciones legales, pero sus disposiciones están pensadas esencialmente en el giro de sus negocios y no tanto en la obligación legal de retener datos para suministrar luego al Estado a solicitud, ni para explicar sobre lo que hacen con ellos para fines comerciales y publicitarios. A pesar de las deficiencias, podemos destacar que la descripción que hace Directv en su política de privacidad es la más detallada.
- En cuanto a la retención de datos y acceso por parte del sector público a nuestra información, en 2018 lo que vimos es que las empresas que han desarrollado informes de transparencia locales –ETB, Claro, Telefónica-Movistar y Tigo-UNE– son las que están yendo más allá de su compromiso con la ley de protección de datos para ofrecernos más transparencia en sus actividades. Estas empresas hacen expreso el marco legal que las obliga frente al sector público. Aunque no son explícitas en decir que hacen retención legal y los plazos al listar las normas que aplican, indicar las autoridades que hacen uso de ellas, el tipo de información que requieren y el tipo de acciones que se dan (evidenciando que sus datos e infraestructura se usan para interceptación de comunicaciones y solicitud de metadatos), nos permite a quienes usamos sus servicios conocer la complejidad de estas actividades.

Políticas de género

- En 2018, cinco de las siete empresas cuentan con una política de compromiso con la igualdad de género que está publicada en su sitio web. Aunque en general el puntaje disminuyó respecto de 2017 debido a que se hizo más estricta la metodología de calificación, es de resaltar que tan solo Emcali y Telebucaramanga aún no obtienen puntaje relacionado con este punto de la evaluación.

10 Esto se conoce como "retención y conservación de datos de personas". Consiste en la obligación legal que tienen las empresas proveedoras de servicios de internet de almacenar diferentes datos personales de sus clientes. Esos datos involucran el uso que le dan a los servicios de telecomunicaciones, así como la ubicación geográfica de sus celulares. Esta información debe ser conservada por cinco años y debe ser entregada a las autoridades correspondientes para fines de investigación criminal y labores de inteligencia. Es importante considerar que estas empresas también guardan datos para propósitos propios de la prestación del servicio y comerciales. Para mayor información, revise las obligaciones del artículo 44 de la Ley 1621 de 2013 y del Decreto 1704 de 2011. *Véase*, además, Castañeda, J.D. (2015, 28 de febrero). La retención de datos en Colombia, una de las más largas del mundo. *Digital Rights Latin America and the Caribbean*. Disponible en https://www.digitalrightslac.net/es/la-retencion-de-datos-en-colombia-una-de-las-mas-largas-del-mundo/ o los *Principios necesarios y proporcionales*, *op. cit.* (nota 6).

Accesibilidad

- En materia del compromiso con la accesibilidad que permita a más personas conocer la información que ofrecen sobre sus servicios, incluyendo a poblaciones con discapacidad, a Telefónica-Movistar, que en 2017, obtuvo la mejor calificación se suman en 2018 Telebucaramanga y Emcali, las dos empresas nacionales más pequeñas de las evaluadas. Telefónica hace un esfuerzo por difundir la política pública de accesibilidad del MinTIC que consiste en impulsar y dar a conocer la oferta que tiene el Estado de un software gratuito que le permite a las personas con discapacidad visual acceder a los contenidos que se encuentran en internet. Telebucaramanga y Emcali tienen una estrategia similar, pero con otros software que han dispuesto en su portal para que las personas con discapacidad pueden usar y conocer la información que ofrecen allí.

Bloqueo de contenidos

- Mientras en 2017 tan solo ETB lo hacía, en 2018, Claro, Telefónica-Movistar y Tigo-UNE también publican información para explicar las medidas que implementan para bloquear contenidos por orden del Gobierno. Si se cuenta con más y mejor información sobre esto se protege la libertad de expresión, pues se nos permite analizar cómo suceden los bloqueos y si el proceso puede prestarse para abusos en la aplicación de las normas asociadas con ellos.
- En 2018 todas las empresas afirman que los bloqueos que adelantan están relacionados con contenidos de explotación sexual infantil, algunas mencionan órdenes judiciales y bloqueos relacionados con juegos de suerte y azar, incluso nos enteramos que también hay una norma que permite suspensiones geográficas o temporales de internet en casos de emergencia, conmoción o calamidad y prevención.
- La información que suministren las PSI sobre el procedimiento que siguen en todos los casos de bloqueos permite establecer si la restricción cumple estándares internacionales y permite que ellas adopten las necesarias garantías en su implementación. De la información que publicaron las empresas en 2018 sobre este tema, se puede deducir que el procedimiento está especialmente claro en lo relacionado con material de explotación sexual infantil, pero es mucho menos claro respecto de las otras dos justificaciones mencionadas. A pesar de ello, la evaluación permite establecer que los procedimientos desarrollados por el Estado están siendo insuficientes en la protección de estándares internacionales de derechos humanos como el debido proceso.
- La importancia de conocer esta información radica en la posibilidad que nos da a las personas usuarias de identificar problemas. Por ejemplo aunque hay más información sobre el bloqueo de material de explotación infantil, no se encuen-

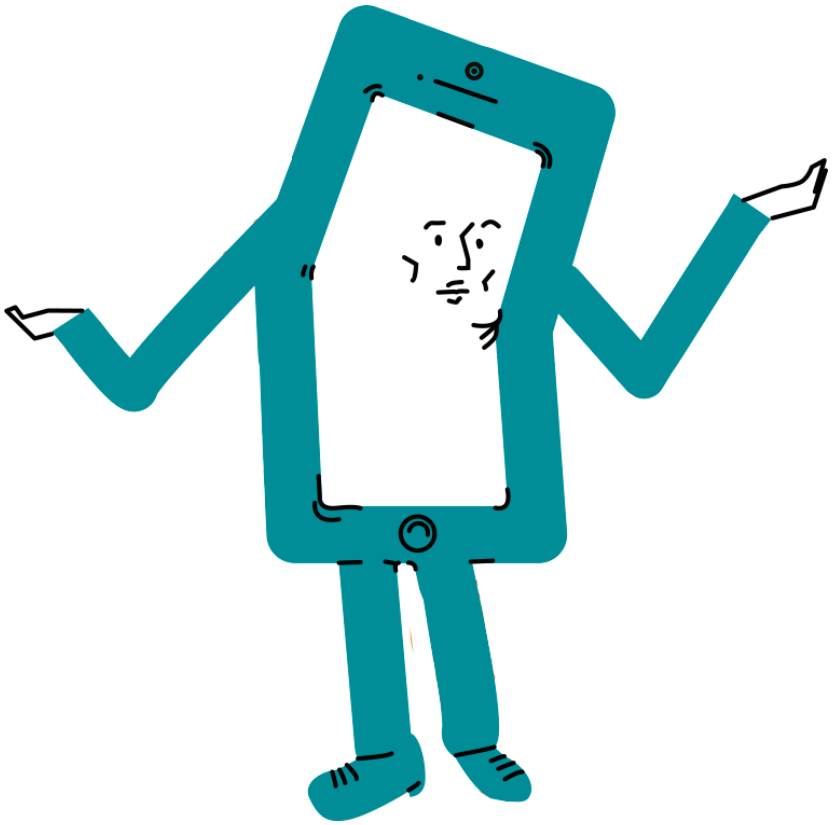
tran mecanismos de corrección de errores, por tanto, una vez se bloquea un sitio por este motivo nadie puede protestar o pedir corrección. En lo relacionado con la información sobre cómo se dan los bloqueos por órdenes judiciales o en casos de emergencia, es todavía muy escasa para permitirnos arribar a conclusiones.

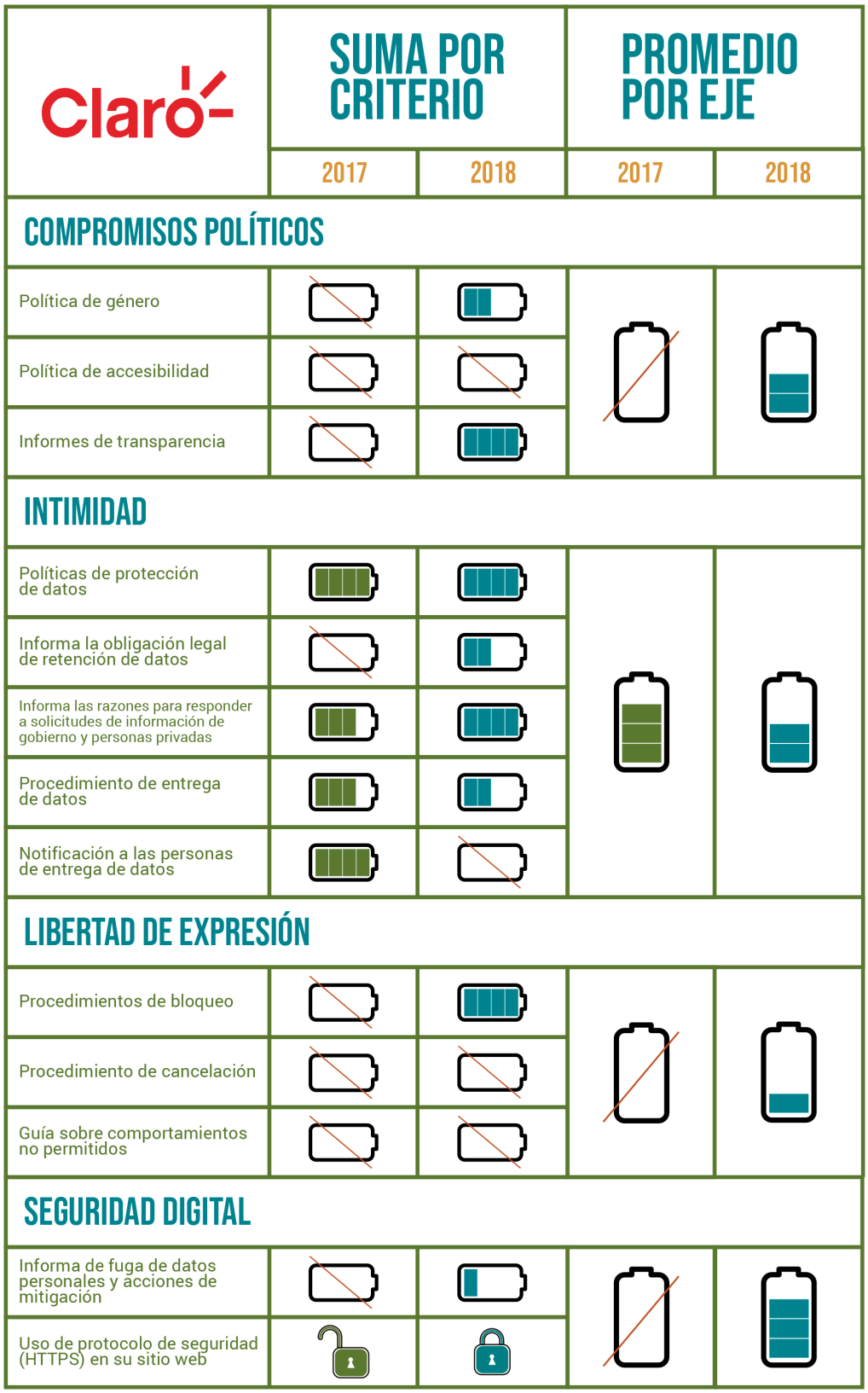
- En el caso de los juegos de azar, lo que podemos deducir es que se ha desarrollado un procedimiento a la sombra del que busca controlar el contenido de explotación sexual de menores pero, no hay suficiente información para afirmar si tiene sus fortalezas y debilidades.
- Se debe elogiar que en el informe de transparencia de Telefónica-Movistar, que es el de su matriz, se monitorea si se dan suspensiones geográficas o temporales del servicio. Este informe da cuenta que, en el periodo reportado, esto no ha sucedido en Colombia. La inclusión de esta información es una alerta a la ciudadanía, en la medida en que nos advierte que existe esa otra justificación de bloqueo que forma parte de las facultades legales del Estado para restringir nuestra libertad de expresión. Sin embargo, quedan sin respuestas las siguientes interrogantes: ¿cuál es el procedimiento que se aplica para activar esta medida?, ¿quién es la autoridad que lo ordenaría?, ¿cómo lo haría?
- Como en años anteriores, ETB desarrolla su compromiso con la libertad de expresión, ofreciendo guías sobre comportamientos no permitidos. Además, sus políticas sobre usos aceptables permiten a las personas saber los parámetros de los servicios y, en consecuencia, entender cuándo pueden ser cancelados o suspendidos. En 2018, Tigo-UNE siguió este mismo ejemplo.

Seguridad

- Con excepción de Emcali y Telefónica-Movistar, las demás empresas evaluadas, aplican el protocolo HTTPS de manera predeterminada en sus sitios web. Esta es la medida mínima de seguridad digital que se debe adoptar en internet para proteger los datos de las personas que interactúan con sitios web.
- Aunque todavía hay mucho por hacer, Claro, ETB, Tigo-UNE, y Telebucaramanga, manifiestan que ven las brechas de seguridad como una amenaza digital. Algunas incluso tienen información sobre formas de mitigarlas, pero en su mayoría se refieren a actos de prevención y no a su compromiso con lo que hacen si la brecha digital sucede.
- La *Ley de protección de datos* obliga a las empresas a informar sobre sus brechas de seguridad. Nuestra evaluación va más allá, analizamos cómo dicen que cumplen el compromiso y, además, que indiquen cómo actuarían para mitigar el impacto de esas brechas de seguridad. Vale la pena aclarar que no analizamos si efectivamente cumplen con esta obligación legal. Sin embargo, lo que se busca es reconocer que no hay seguridad al ciento por ciento, que queremos saber cómo

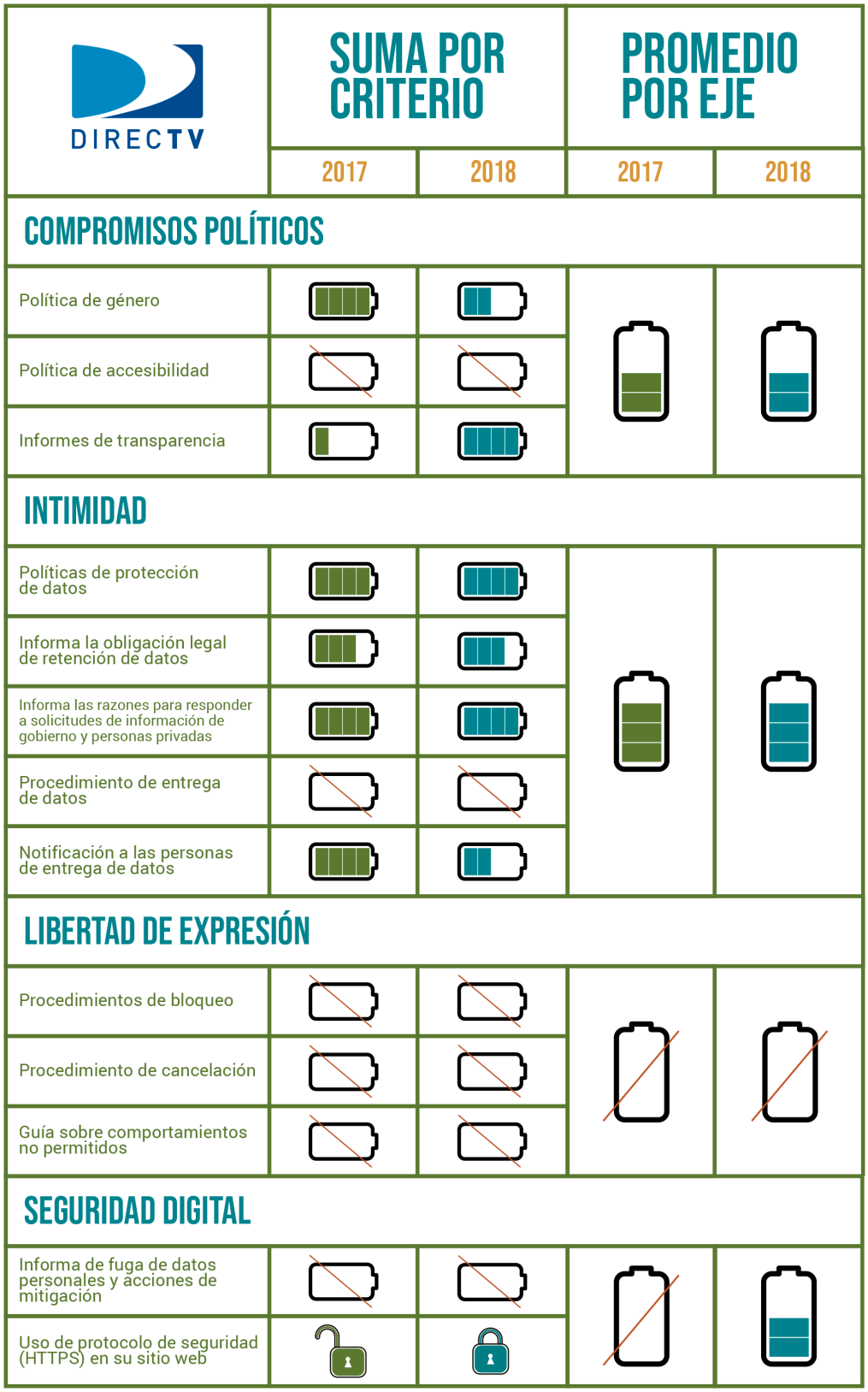
actuarían si esa eventualidad ocurriera. Creemos que las reformas recientes en Europa mejorar las prácticas comerciales en este ámbito. Es probable que pronto las empresas empiecen a hacer modificaciones en línea con estos criterios de evaluación a nivel internacional y se comprometan a avisar a las autoridades –no solo de protección de datos, sino aquellas vinculadas con la seguridad digital– en plazos breves. Esto también podría llevar al desarrollo de protocolos de notificación a las personas afectadas y para mitigar riesgos.

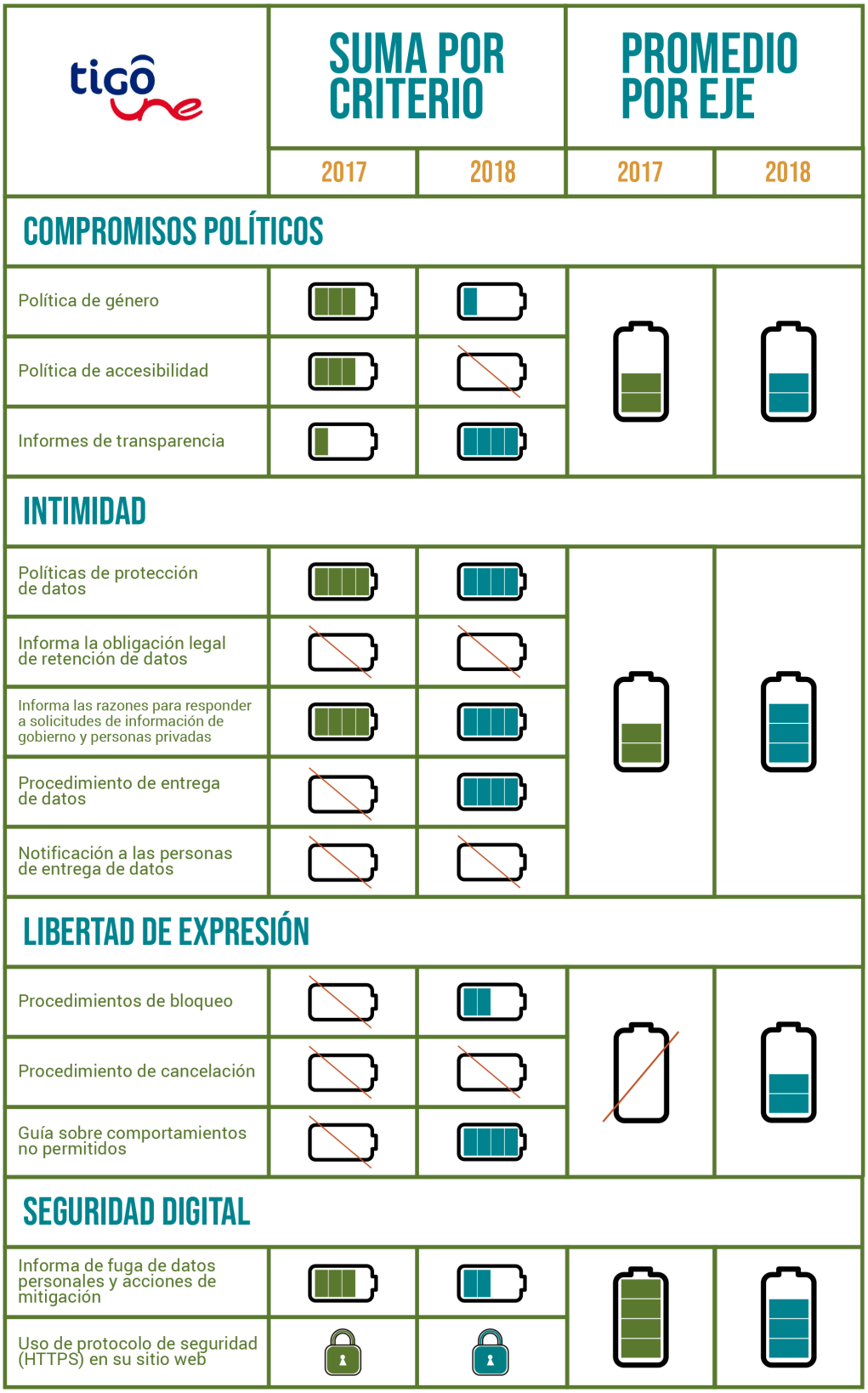



Claro
SUMA POR CRITERIO
PROMEDIO POR EJE
2017
2018
2017
2018
COMPROMISOS POLÍTICOS
Política de género
Política de accesibilidad
Informes de transparencia
INTIMIDAD
Políticas de protección de datos
Informa la obligación legal de retención de datos
Informa las razones para responder a solicitudes de información de gobierno y personas privadas
Procedimiento de entrega de datos
Notificación a las personas de entrega de datos
LIBERTAD DE EXPRESIÓN
Procedimientos de bloqueo
Procedimiento de cancelación
Guía sobre comportamientos no permitidos
SEGURIDAD DIGITAL
Informa de fuga de datos personales y acciones de mitigación
Uso de protocolo de seguridad (HTTPS) en su sitio web

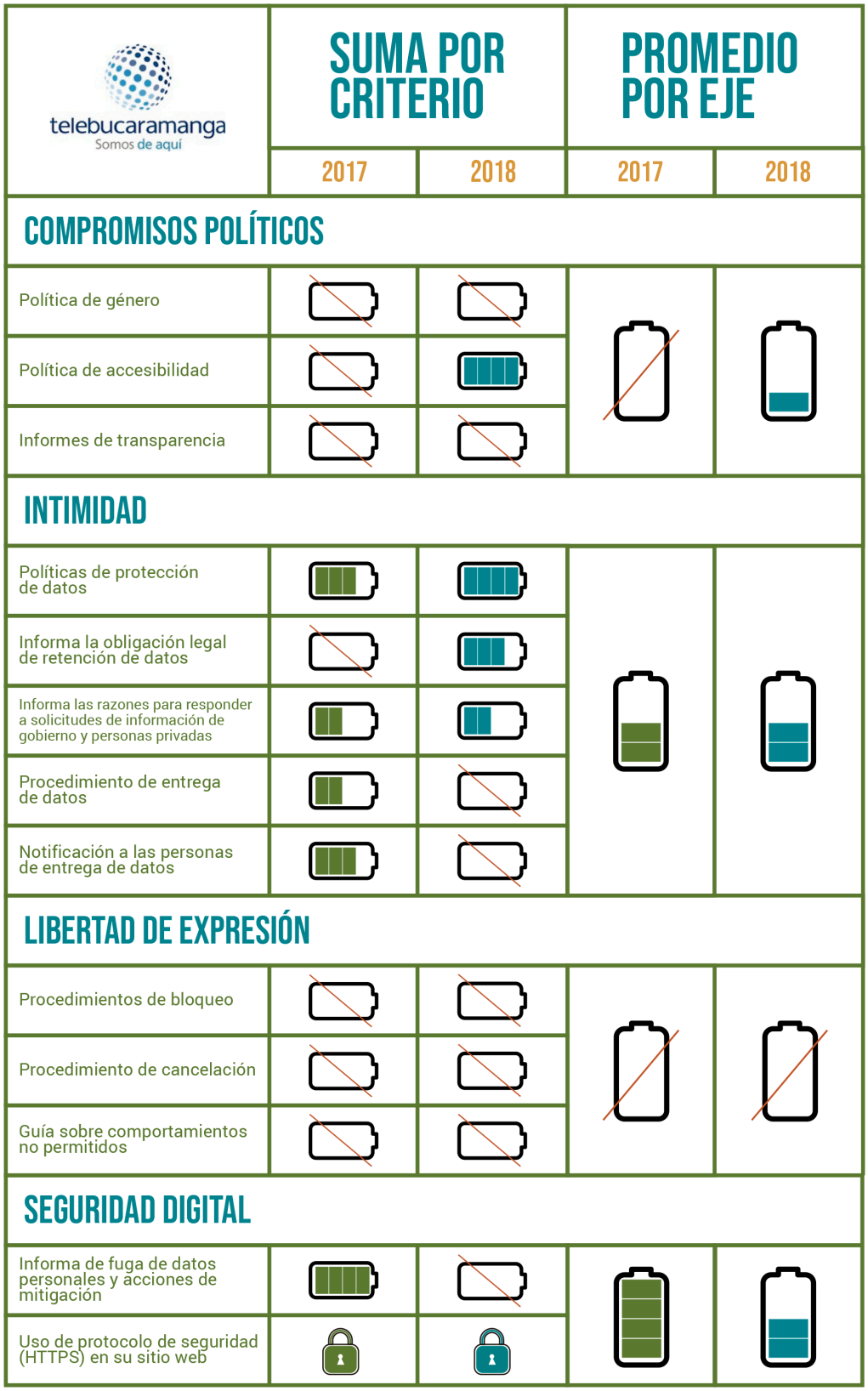
Telefónica	SUMA POR CRITERIO		PROMEDIO POR EJE	
	2017	2018	2017	2018
COMPROMISOS POLÍTICOS				
Política de género				
Política de accesibilidad				
Informes de transparencia				
INTIMIDAD				
Políticas de protección de datos				
Informa la obligación legal de retención de datos				
Informa las razones para responder a solicitudes de información de gobierno y personas privadas				
Procedimiento de entrega de datos				
Notificación a las personas de entrega de datos				
LIBERTAD DE EXPRESIÓN				
Procedimientos de bloqueo				
Procedimiento de cancelación				
Guía sobre comportamientos no permitidos				
SEGURIDAD DIGITAL				
Informa de fuga de datos personales y acciones de mitigación				
Uso de protocolo de seguridad (HTTPS) en su sitio web				

eTb	SUMA POR CRITERIO		PROMEDIO POR EJE	
	2017	2018	2017	2018
COMPROMISOS POLÍTICOS				
Política de género				
Política de accesibilidad				
Informes de transparencia				
INTIMIDAD				
Políticas de protección de datos				
Informa la obligación legal de retención de datos				
Informa las razones para responder a solicitudes de información de gobierno y personas privadas				
Procedimiento de entrega de datos				
Notificación a las personas de entrega de datos				
LIBERTAD DE EXPRESIÓN				
Procedimientos de bloqueo				
Procedimiento de cancelación				
Guía sobre comportamientos no permitidos				
SEGURIDAD DIGITAL				
Informa de fuga de datos personales y acciones de mitigación				
Uso de protocolo de seguridad (HTTPS) en su sitio web				


DIRECTV
SUMA POR CRITERIO
PROMEDIO POR EJE
2017
2018
2017
2018
COMPROMISOS POLÍTICOS
Política de género
Política de accesibilidad
Informes de transparencia
INTIMIDAD
Políticas de protección de datos
Informa la obligación legal de retención de datos
Informa las razones para responder a solicitudes de información de gobierno y personas privadas
Procedimiento de entrega de datos
Notificación a las personas de entrega de datos
LIBERTAD DE EXPRESIÓN
Procedimientos de bloqueo
Procedimiento de cancelación
Guía sobre comportamientos no permitidos
SEGURIDAD DIGITAL
Informa de fuga de datos personales y acciones de mitigación
Uso de protocolo de seguridad (HTTPS) en su sitio web


tigo une
SUMA POR CRITERIO
PROMEDIO POR EJE
2017
2018
2017
2018
COMPROMISOS POLÍTICOS
Política de género
Política de accesibilidad
Informes de transparencia
INTIMIDAD
Políticas de protección de datos
Informa la obligación legal de retención de datos
Informa las razones para responder a solicitudes de información de gobierno y personas privadas
Procedimiento de entrega de datos
Notificación a las personas de entrega de datos
LIBERTAD DE EXPRESIÓN
Procedimientos de bloqueo
Procedimiento de cancelación
Guía sobre comportamientos no permitidos
SEGURIDAD DIGITAL
Informa de fuga de datos personales y acciones de mitigación
Uso de protocolo de seguridad (HTTPS) en su sitio web

EMCALI	SUMA POR CRITERIO		PROMEDIO POR EJE	
	2017	2018	2017	2018
COMPROMISOS POLÍTICOS				
Política de género				
Política de accesibilidad				
Informes de transparencia				
INTIMIDAD				
Políticas de protección de datos				
Informa la obligación legal de retención de datos				
Informa las razones para responder a solicitudes de información de gobierno y personas privadas				
Procedimiento de entrega de datos				
Notificación a las personas de entrega de datos				
LIBERTAD DE EXPRESIÓN				
Procedimientos de bloqueo				
Procedimiento de cancelación				
Guía sobre comportamientos no permitidos				
SEGURIDAD DIGITAL				
Informa de fuga de datos personales y acciones de mitigación				
Uso de protocolo de seguridad (HTTPS) en su sitio web				



telebucaramanga Somos de aquí	SUMA POR CRITERIO		PROMEDIO POR EJE	
	2017	2018	2017	2018
COMPROMISOS POLÍTICOS				
Política de género				
Política de accesibilidad				
Informes de transparencia				
INTIMIDAD				
Políticas de protección de datos				
Informa la obligación legal de retención de datos				
Informa las razones para responder a solicitudes de información de gobierno y personas privadas				
Procedimiento de entrega de datos				
Notificación a las personas de entrega de datos				
LIBERTAD DE EXPRESIÓN				
Procedimientos de bloqueo				
Procedimiento de cancelación				
Guía sobre comportamientos no permitidos				
SEGURIDAD DIGITAL				
Informa de fuga de datos personales y acciones de mitigación				
Uso de protocolo de seguridad (HTTPS) en su sitio web				

LOS RESULTADOS COMPARADOS DE 2018

Con los datos que presentamos en este documento, podemos afirmar que las políticas de las empresas que proveen servicios de conexión a internet han mejorado en Colombia. También se debe reconocer que ha aumentado el interés de estas instituciones por mejorar sus prácticas y tener un diálogo más abierto con organizaciones como Karisma, al reconocer que es una herramienta para mejorar sus prácticas comerciales en sintonía con sus compromisos de derechos humanos.

Si esta investigación tuvo como motor inicial conseguir que las empresas colombianas se alinearan con la buena práctica internacional de publicar informes de transparencia, esta cuarta versión del informe ¿Dónde están mis datos? puede afirmar el éxito de este objetivo trazado inicialmente en 2015. Esto nos impone un nuevo reto. Seguramente a partir de 2019, trabajaremos para mejorar el tipo de información que se nos suministra, de modo que, estos datos sirvan para propósitos de control ciudadano, especialmente para hacer seguimiento y control a la facultad del Estado de pedir información de las personas.

Si las empresas ofrecen más y mejor información sobre sus propias políticas para proteger y respetar los derechos a la libertad de expresión y a la intimidad y nos dan más datos sobre cómo deben cumplir frente a las regulaciones, se mejoran nuestras garantías en el ejercicio de estos derechos, se fortalece nuestra capacidad para exigir efectividad. Todavía se puede mejorar, pero el camino recorrido es importante.

I. TRANSPARENCIA

Alrededor del mundo las empresas que ofrecen servicios de internet han estado implementando informes de transparencia, con el fin de entregar a las personas información sobre la forma como cumplen con las normas legales de suministro de datos por requerimiento de las autoridades. Esta información es muy importante para que la sociedad

civil pueda hacer un control independiente de las actuaciones del Estado y para evitar que entren en conflicto con estándares internacionales de derechos humanos.

De las siete empresas evaluadas, cuatro forman parte de multinacionales. Tres de las matrices de esas multinacionales, Millicom (Tigo-UNE), AT&T (Directv) y Telefónica (Telefónica-Movistar), publican informes de transparencia adoptando esta buena práctica internacional. América Móvil (Claro) aún no lo hace. Sin embargo, América Móvil México está obligada legalmente a presentar informes anuales de transparencia. La buena práctica global, que se ha convertido en un ejemplo mundial, en 2018 se puede decir que ha llegado a Colombia, al menos en el sector de las telecomunicaciones.

Este es el aspecto que más ha cambiado desde que se comenzó esta investigación y se hizo el primer informe en 2015. Al principio ninguna de las empresas evaluadas cumplía con esta buena práctica, en 2018, cinco de las siete empresas lo hacen.

ETB publicó por primera vez información de este tipo en 2016 y así lo reconocimos en la versión de 2017 de este informe. El primer reconocimiento que se debe hacer a esta empresa es el hecho de que es una empresa nacional que no tiene vínculos internacionales, por tanto, no tiene ejemplos de sus matrices como podría decirse de otros casos.

Las cinco empresas que publicaron informes de transparencia o información equivalente, obtuvieron en 2018 la totalidad del puntaje al cumplir con el criterio de evaluación.

Sobre las políticas de igualdad de género, las cinco empresas más grandes las contemplan de una u otra forma, siendo Telefónica la mejor calificada.

En relación con las políticas de accesibilidad, Telefónica, Emcali y Telebucaramanga se llevaron los 4 puntos porque facilitan la accesibilidad de su información a las personas con discapacidad en forma efectiva. Telefónica está facilitando el software que MinTiC ha adquirido para que cualquier persona en Colombia con discapacidad visual pueda acceder a sitios y materiales digitales; mientras que Emcali y Telebucaramanga disponen también de un aplicativo en su portal con el que las personas con discapacidad pueden usar y conocer la información allí disponible. Si bien estas no son políticas en concreto, puede que incluso sea mejor, pues, proveen la herramienta para hacer efectiva la accesibilidad.

En Karisma creemos que implementar políticas corporativas en estos temas incrementa las posibilidades de que la tecnología sea un factor de desarrollo y que sirva de herramienta para favorecer el ejercicio de derechos humanos en ambientes diversos.

Finalmente, por segundo año consecutivo, Karisma propone dar bonificación a las empresas que intenten adoptar en sus políticas lenguaje incluyente. Sabemos que no es un tema fácil y tampoco suele ser bien recibido. El lenguaje construye imaginarios, por lo que es importante empezar a cuestionarse cómo lo utilizamos y cómo representamos a

las personas. Si bien reconocemos que usar lenguaje inclusivo es un proceso complejo y lleno de dificultades, es un esfuerzo que invitamos a las empresas a hacer y premiamos. Sabemos que se puede hacer. Sin embargo, la diversidad exige que intentemos identificar formas de lograr el efecto incluyente, incluso en el lenguaje. Esperamos que este sea un incentivo para intentar un ensayo de este tipo. Tanto en 2017 como en 2018 esta bonificación se la ha llevado Telefónica puesto que en su política de género hace un esfuerzo por desarrollar este lenguaje.

II. INTIMIDAD

En las primeras dos evaluaciones de ¿Dónde están mis datos? nos sorprendió ver cómo las políticas de protección de datos de las empresas eran documentos legales, descritos en forma compleja para la población común y usando formatos técnicos que no permitían su reutilización. Para 2017, la evolución de los documentos en las cinco empresas evaluadas desde el primer informe era importante, para 2018 las siete empresas evaluadas cuentan con documentos mucho más amigables y comprensibles para cualquier persona. Algunas empresas incluso han desarrollado espacios autónomos que facilitan la experiencia de uso y facilitan el acceso a la información. Mención especial en este sentido merece Telefónica-Movistar.

En las primeras evaluaciones también nos sorprendió lo difícil que podía ser llegar a estos documentos. En algunos casos se requerían hasta de 7 pasos para encontrarlos. Hoy la mayoría están a dos enlaces de distancia de su página principal. La oportunidad más importante para mejorar este aspecto la tienen ETB y Emcali, que tuvieron una calificación más baja en este criterio concreto –aunque por la metodología de aproximación a la unidad no les afectó el promedio del eje temático–, puesto que se requieren más de dos pasos para descubrir el documento, haciendo que no sea fácil encontrarlo.

En relación con el segundo y tercer criterio de evaluación de este eje temático, las empresas han ido mejorando la información sobre la obligación legal de retención de datos. Si las empresas guardan nuestros datos, lo siguiente que puede suceder es que les hagan solicitudes o requerimientos para conocer estos datos. Los requerimientos pueden ser legales –provenientes de autoridades y que son de obligatorio cumplimiento–, o vinculados con las actividades de la empresa –para facturar los servicios o conocer mejor a sus clientes–, o relacionados con compromisos contractuales como los que adquieren las empresas en desarrollo de actividades comerciales como tarjetas de fidelidad o compra-venta de bases de datos para campañas comerciales.

Que las empresas expliquen mejor la forma como cumplen tanto con sus obligaciones legales de retención de datos como de entrega de los mismos y, en general, que describan la forma como guardan estos datos y los gestionan, permite a las personas

dimensionar mejor las actividades y los riesgos que entrañan. En 2018, la mejora fue significativa respecto de la obligación legal, en especial, asociada con los informes de transparencia, puesto que, en su mayoría, incluyen el marco legal y el tipo de datos que se retienen. También de estos informes se deducen las razones de las solicitudes y se establecen las autoridades que los hacen. Sin embargo, aún hay espacio para dar más y mejor información.

En cuanto al cuarto criterio de este eje temático relacionado con la publicación del procedimiento para entrega de nuestra información a petición de parte, la información suministrada en los informes de transparencia le sirvieron a Claro y a Telefónica-Movistar para ganar algo de puntos. Sin embargo, la mejor evaluación se la llevaron ETB y Tigo-UNE, empresas que hicieron esfuerzos expresos por publicar sus procedimientos, la primera en función de la interceptación de comunicaciones y la segunda en relación con la entrega de metadatos.

Finalmente, conseguir que las empresas se comprometan a notificar a las personas siempre que alguien solicite información sobre ellas es muy importante en la defensa de la intimidad. Para garantizar el debido proceso y el derecho a la defensa en casos de vigilancia de las comunicaciones, la persona que está siendo sujeta a vigilancia debe ser notificada de la decisión. Para evitar abusos en los requerimientos de información personal, también debe informarse a la persona titular de los datos entregados. Esto le permite a la persona afectada defenderse o buscar otra solución.

Esta disposición no es expresa en Colombia, pero tampoco hay una norma que diga que no puede hacerse. En cambio, de acuerdo con los estándares internacionales de derechos humanos, la notificación es la regla, tanto así que la demora en realizar esta notificación debe ser excepcional y justificada.[11] Aunque es una obligación del Estado, las empresas proveedoras pueden hacerlo por voluntad o a petición, precisamente, como un compromiso con la defensa del derecho a la intimidad de quienes confían en ellas sus datos.

III. LIBERTAD DE EXPRESIÓN

Estamos viendo una preocupante tendencia en el mundo en donde los gobiernos presionan a las empresas proveedoras de internet para que bloqueen, corten contenidos, URL, servicios de internet o cuentas. Probablemente, estas acciones incrementarían de varias formas: desde cortes generales de internet a la población hasta bloqueos selectivos para evitar que las personas accedan a aplicativos o contenidos determinados.

11 De acuerdo a los *Principios necesarios y proporcionales*, la demora en notificar se justifica cuando se pone en peligro la finalidad para la que se autoriza la vigilancia, peligra una vida humana, o porque la propia autoridad judicial así lo define. *Véase* el Principio No. 8, disponible en https://necessaryandproportionate.org/es/necesarios-proporcionados.

La libertad de expresión supone que las personas puedan informar e informarse libremente. Esta libertad se limita cuando el Estado obliga a los PSI a bloquear contenidos, Por eso hacer seguimiento y control a la forma como se desarrollan e implementan estas facultades busca asegurarnos que se incorporen las necesarias garantías.

En 2018 logramos establecer que el Estado no está cumpliendo con estándares internacionales que lo obligan, pues toda limitación a la libertad de expresión –como lo es una disposición de bloqueo de cualquier tipo que impone a las empresas que nos proveen servicios de internet– sea necesaria, legal y proporcional. Las empresas están bloqueando contenidos no solo en desarrollo de su obligación de protección a niños, niñas y adolescentes[12] --para evitar que se distribuya contenido sexual que les involucre--, también por órdenes judiciales, por apuestas ilegales[13] y estarían obligadas a hacer suspensiones geográficas o temporales del servicio en casos de emergencia, conmoción o calamidad y prevención. Algunas de estas empresas ofrecen información sobre los procedimientos que usan en el caso de contenidos de explotación sexual de menores, pero en los demás casos no existe información suficiente sobre los procedimientos. Hasta donde ha podido llegar la investigación de Karisma, podríamos afirmar que no se cumple con la garantía del debido proceso, ya que que no es posible denunciar o corregir errores en los bloqueos, por ejemplo.

En 2018, la información suministrada en relación con el procedimiento que siguen para los bloqueos significó el máximo puntaje para Claro, ETB y Telefónica-Movistar.

En relación con procedimientos de cancelación, la única que obtiene puntaje este año, como sucedió en el anterior, es ETB. Sobre comportamientos no permitidos, ETB comparte este año el mayor puntaje con Tigo-UNE.

IV. SEGURIDAD DIGITAL

Las personas pueden tener comportamientos y adoptar herramientas más seguras, pero creemos que las empresas proveedoras de internet pueden también implementar medidas más seguras, reconocer que no hay seguridad digital perfecta y, por tanto, informar sobre la forma como mitigan las brechas de seguridad que se pueden presentar. Se trata de trabajar en la construcción de confianza, que es una buena medida para mejorar la seguridad digital.

12 *Véase* la Ley 679 de 3 de agosto de 2001 y el Decreto 1524 de 23 de julio de 2002.

13 *Véase* por ejemplo el artículo "Durante la versión 32 de Andicom el ministro Luna habló sobre la polémica frente a la operación de la compañía" en el Diario La República que cita al entonces Ministro TIC David Luna en agosto 2017 https://www.larepublica.co/economia/david-luna-anuncio-que-el-ministerio-tic-no-bloqueara-plataformas-como-uber-2539657

Adicionalmente, si bien en Colombia la *Ley de protección de datos* prevé que las empresas informen de fugas de datos, no se trata de una obligación muy detallada. Esto seguramente cambiará en un futuro cercano. La nueva *Directiva europea de protección de datos* (GDPR, por sus siglas en inglés) o las políticas que están desarrollando el Ministerio de las TIC y la Comisión de Regulación de Comunicaciones tienen previsiones más detalladas al respecto. Además, las empresas están entendiendo que la construcción de confianza con las personas pasa por ampliar sus compromisos de transparencia y seguridad digital.

En 2018, se evalúa por segunda vez ese eje temático y la evolución es muy positiva. Tigo-UNE es la empresa que más y mejor información da sobre brechas de seguridad. En relación con la implementación del protocolo seguro de transmisión de datos HTTPS, todas las empresas lo implementan como predeterminado, menos Telefónica-Movistar y Emcali. Directv arroja en el test que lo hace, pero encontramos que los documentos utilizados para la investigación no lo incluía. Esta es una de esas raras excepciones en las que la evaluación de los compromisos nos hace ver fallas en la práctica o implementación del mismo por la empresa, de modo que, castigamos el puntaje. Es excepcional porque la metodología no permite evaluar sino el compromiso, ya que Karisma en esa investigación no busca activamente establecer si, efectivamente, se cumple o no con lo que se promete.

LA EVALUACIÓN DE CADA EMPRESA

Los detalles de la evaluación que efectuamos durante la primera mitad del mes de octubre de 2018 a los sitios web de cada empresa y nuestra lectura de esos resultados se describen a continuación:

Claro	PUBLICIDAD	CLARIDAD	FACILIDAD	ACCESIBILIDAD	LENGUAJE INCLUSIVO (BONIFICACIÓN)	SUMA POR CRITERIO	PROMEDIO POR EJE
COMPROMISOS POLÍTICOS							
Política de género	0,6	0,6	0,3	0,3		2	2
Política de accesibilidad						0	
Informes de transparencia	1	1	1	1		4	
INTIMIDAD							
Políticas de protección de datos	1	1	1	1	0	4	2
Informa la obligación legal de retención de datos	0,33	0,33	0,33	0,33	0,33	2	
Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	1	1	1	0	4	
Procedimiento de entrega de datos	0,5	0,5	0,5	0,5	0	2	
Notificación a las personas de entrega de datos					0	0	
LIBERTAD DE EXPRESIÓN							
Procedimientos de bloqueo	1	1	1	1		4	1
Procedimiento de cancelación						0	
Guía sobre comportamientos no permitidos						0	
SEGURIDAD DIGITAL							
Informa de fuga de datos personales y acciones de mitigación	0,3	0,3	0,3	0,3		1	3
Uso de protocolo de seguridad (HTTPS) en su sitio web	4					4	

La evaluación de Claro mejora sustancialmente en tres de los 4 ejes temáticos evaluados respecto del resultado del año anterior. El área de intimidad disminuye debido a que se hizo más estricta la calificación este año; no significa que el compromiso de la empresa hubiese bajado.

COMPROMISOS POLÍTICOS

El primer cambio que se presenta en 2018 se debe al Código de Ética de América Móvil. En su capítulo de "Respeto a los Derechos Humanos y no discriminación", se encuentra la promoción del respeto e inclusión en el lugar de trabajo, no permitir el acoso y la prohibición de imágenes u objetos de contenido sexual, entre otros. Pero no hace referencia a desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos; tampoco al equilibrio familiar-laboral.

El segundo cambio importante tiene que ver con la publicación de su primer informe de transparencia para Colombia. Claro publicó un aparte dentro de su informe de sostenibilidad que constituye su informe de transparencia. Esto debe ser reconocido como un avance importante para fortalecer la transparencia y mejorar la capacidad de quienes se suscriben a sus servicios de comprender lo que sucede con estos. En este informe se detalla el contexto legal de las solicitudes de información personal de 2017 y los bloqueos o restricciones de contenidos.

El contexto que ofrece Claro sobre autoridades y marco legal es de resaltar, aunque creemos que sería muy positivo que se entregaran más detalles en cifras para saber el tipo de solicitudes que recibe y, por ejemplo, cuántas son atendidas.

INTIMIDAD

Claro cuenta con una política de protección de datos que se descarga desde su página principal. Se trata de un documento que cumple con los requerimientos de la evaluación.

Las políticas de protección de datos de Claro indican que la recolección de datos que hace está sujeta a la ley, y que los datos personales que recoge son los "pertinentes y adecuados". En su informe de transparencia también describe el marco legal que le aplica. No obstante, en sus políticas, Claro no informa sobre el tipo de datos que recoge y no habla del tiempo de retención expresamente, ni en lo referente al sector público ni en el giro normal de su negocio.

En el tercer ítem de calificación que consiste en "informar las razones para responder a solicitudes de información del sector público y personas privadas", Claro informa en su política que el tratamiento de datos lo hace con fines comerciales y publicitarios. Creemos podría explicar mejor el alcance de esta actividad. En lo relacionado con el sector público, la empresa detalla en su informe de transparencia que está obligado, respecto de diferentes autoridades, por las normas de interceptación de comunicaciones y de entrega de datos personales de quienes usan sus servicios.

Claro no cuenta con ningún documento que describa o detalle el "Procedimiento de entrega de datos al sector público y empresas privadas". Sin embargo, en el informe de transparencia hace un esfuerzo por explicar el tipo de solicitudes que atiende, las autoridades que reconoce como legitimadas para hacerlas y el marco legal que aplica. El esfuerzo puede mejorarse para explicar internamente como lo implementa de modo que se pueda establecer si se respetan garantías como la del debido proceso. Este esfuerzo se reconoció en la calificación.

De otra parte, la empresa reconoce que dará información a la persona que la solicite sobre cómo se usan sus datos. Sin embargo, lo que se califica en esta evaluación es si la empresa se compromete a notificar activamente cuando entrega sus datos a solicitud de otro, sobre todo cuando se deriva de una obligación legal o judicial, por eso no se reconoce ningún punto en este tema.

LIBERTAD DE EXPRESIÓN

En su Código de Ética, Claro establece un compromiso con la libertad de expresión y señala que puede restringir contenido cuando la legislación interna lo requiera. En su informe de transparencia detalla el procedimiento que aplica para los bloqueos legales que describe más allá de los relacionados con materiales de explotación infantil. También explica los que son resultado de apuestas ilegales y de órdenes judiciales. En este documento se describe el marco legal, las autoridades competentes y el procedimiento que aplican. El documento constituye un gran avance frente a lo que se tenía en 2017.

Claro no obtiene puntos en los otros dos criterios, porque no se identificaron documentos que los desarrollaran.

SEGURIDAD DIGITAL

En el ítem de "Informa de fuga de datos personales y acciones de mitigación", se evalúan tres componentes. En la información pública de Claro, solo se encuentra la notificación a las autoridades competentes, específicamente a la Superintendencia de Industria y Comercio, que se ha reconocido como positivo. Aunque se encontraron documentos que se refieren a la prevención de brechas de seguridad por parte de la empresa y de las personas usuarias, no se menciona un procedimiento de respuesta a este tipo de incidentes que incluyera el compromiso de informar sin demora a las autoridades, de notificar a los afectados, ni una descripción sobre cómo mitigaría los daños.

Una evaluación en el portal de SSLabs estableció que Claro ha desplegado como predeterminado el protocolo de seguridad HTTPS en su sitio web. Esto es un cambio sustancial frente a lo que se había visto en 2017.

La calificación de Telefónica en 2018 mejora en 3 de los 4 ejes temáticos evaluados respecto del puntaje obtenido el año anterior. La otra área mantiene el mismo puntaje.

Telefónica	PUBLICIDAD	CLARIDAD	FACILIDAD	ACCESIBILIDAD	LENGUAJE INCLUSIVO (BONIFICACION)	SUMA POR CRITERIO	PROMEDIO POR EJE
COMPROMISOS POLÍTICOS							
Política de género	0,6	0,6	0,6	0,6	1	3	4
Política de accesibilidad	1	1	1	1	0	4	
Informes de transparencia	1	1	1	1		4	
INTIMIDAD							
Políticas de protección de datos	1	1	1	1	0	4	3
Informa la obligación legal de retención de datos	0,66	0,66	0,66	0,66	0	3	
Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	1	1	1	0	4	
Procedimiento de entrega de datos	0,5	0,5	0,5	0,5	0	2	
Notificación a las personas de entrega de datos					0	0	
LIBERTAD DE EXPRESIÓN							
Procedimientos de bloqueo	1	1	1	1		4	3
Procedimiento de cancelación						0	
Guía sobre comportamientos no permitidos	1	1	1	1		4	
SEGURIDAD DIGITAL							
Informa de fuga de datos personales y acciones de mitigación	0,3	0,3	0,3	0,3	0	1	1
Uso de protocolo de seguridad (HTTPS) en su sitio web						0	

COMPROMISOS POLÍTICOS

La política de género cambia por la forma como se hizo más estricta la evaluación. Se debe reconocer que aunque esta empresa forma parte de una multinacional, cuenta con una política de género exclusiva para nuestro país, en la que hace referencia a la necesidad de hacer más incluyentes sus espacios de trabajo, con el fin de evitar el acoso, de garantizar que el porcentaje de mujeres dentro de su planta laboral aumente y que puedan acceder cargos de liderazgo. Telefónica no obtiene el total del puntaje porque su política de igualdad de género y el documento de diversidad solo abordan "selección y contratación de personal (diversidad sexual y de género) y desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos"; faltarían los otros puntos.

Adicionalmente, esta política hace un intento por emplear un lenguaje incluyente que muestra su compromiso con la diversidad. Es la única empresa por dos años consecutivos recibe una bonificación por este hecho.

En relación con la política de accesibilidad, se mantiene la calificación. Aunque no hay expresamente un documento de política, sí se pone a disposición una herramienta que hace efectiva esa accesibilidad. Telefónica-Movistar es la única empresa de las evaluadas que impulsa el software que el Ministerio de las TIC ofrece gratuitamente a cualquiera en Colombia.

Para este período, se califica el informe global de transparencia publicado por Telefónica, la matriz, que incluye apartados sobre los países donde tiene operaciones, incluyendo Colombia en relación con 2017. Este informe tiene mucha más información que la de su predecesor sobre todo en términos de contexto, ofreciendo el marco legal y procedimientos. El informe puede mejorar para ofrecer más detalles de las cifras, indicando el tipo de solicitudes que recibe por parte de terceros, sean autoridades locales o terceros privados; y cuándo, cómo y porqué puede compartir información de las personas que utilizan sus servicios. Este informe se encuentra ahora enlazado desde el sitio web de Telefónica Colombia.

INTIMIDAD

Un esfuerzo a resaltar nuevamente en el caso de Telefónica-Movistar es que creó un sitio web que recoge toda la información sobre los temas de privacidad y seguridad de una manera amigable. Adicionalmente, se resalta que la "Política de protección de datos" mejora en claridad al ser parte de la evaluación "Política Privacidad del Grupo Telefónica", que contribuye a comprender mejor los documentos.

La "Política de Privacidad" de Telefónica expone el tipo de datos que se recopilan y en general se habla de los fines. Pese a que no hay una mención expresa a que tiene una obligación legal de retener datos, la descripción que hace del marco legal en el informe

de transparencia permite hacer esta deducción. Asimismo, respecto del sector público, el informe de transparencia menciona las autoridades que pueden interceptar comunicaciones y pedir información, incluyendo a la Fiscalía. Telefónica-Movistar no indica la forma como aplica los plazos legales de retención de datos, pero manifiesta en forma muy amplia el plazo por el que guarda los datos indicando:

> *Las bases de datos de Colombia Telecomunicaciones tienen vigencia indefinida. Los datos personales recolectados se conservarán por el tiempo que dure la relación existente entre la Empresa y el titular de los datos, y por el tiempo necesario para el cumplimiento de los deberes legales o contractuales que Colombia Telecomunicaciones deba observar."*

En relación con las razones por las que guarda los datos, la política de Telefónica-Movistar, además de referirse al giro ordinario de sus actividades y a la publicidad, menciona que cumple con el marco legal. Ahora bien, es en el informe de transparencia donde desarrolla esa obligación para dar el marco legal e indicar que entrega información personal de las personas a las que da servicios en desarrollo de actividades de interceptación de comunicaciones en líneas fijas (indica expresamente que, sobre las móviles, la Fiscalía realiza directamente estas interceptaciones) y para dar acceso a metadatos.

De otra parte, respecto al criterio sobre procedimiento de entrega de datos, no se encontró ningún documento que explique el procedimiento que realiza la empresa, mucho menos si este tendría en cuenta garantías como el debido proceso. Sin embargo, en su informe de transparencia hace un esfuerzo por indicar el marco legal con el que responde a estas peticiones y describe las autoridades a las que responde estos requerimientos.

Y, por último, en lo relacionado con el criterio de notificación de la entrega de datos, en su política de privacidad, se menciona en el índice 6 que "informa a los interesados de forma clara y sencilla que se recolectan los datos y cómo los utilizan". Sin embargo, esta afirmación no tiene el alcance que se evalúa al no ser un compromiso expreso de informar a las personas siempre que entregue a terceros sus datos.

LIBERTAD DE EXPRESIÓN

El informe de transparencia publicado por la empresa en 2018 confirma que han recibido y realizado procedimientos de bloqueo. También se ofrecen detalles del procedimiento que sigue para bloquear y filtrar determinados contenidos, que incluye las suspensiones geográficas o temporales de servicio, que, si bien están previstas en la ley para casos de emergencia, conmoción o calamidad y prevención, no se usaron en el país en 2017.

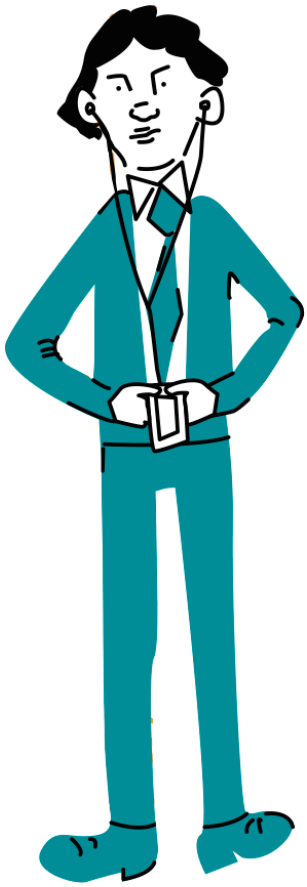
No se encontró información sobre cancelación de cuentas ni una guía de comportamientos no permitidos que permita a las personas que usan sus servicios tener más claridad sobre cómo pueden perder o conservar su calidad de clientes.

SEGURIDAD DIGITAL

En sus políticas, Telefónica señala que avisará a sus clientes de brechas de seguridad, lo que sumó a su calificación. Aunque Telefónica-Movistar cuenta con documentos como la "Política Global de Seguridad" y el "Anexo de Seguridad", que señalan que la empresa está constantemente destinando recursos a mejorar sus servicios de seguridad, ninguno menciona que avisará sin demora, comprometiéndose con plazos máximos, por ejemplo, para notificar de estas brechas a las autoridades. Tampoco indica las medidas o procedimientos para mitigar una brecha. Esto no permite darle a la empresa una calificación de 1 punto.

Por último, esta empresa aún no implementa de manera automática en su portal web el protocolo de transmisión segura de datos HTTPS. Esto se corroboró a través de un *Server Test* realizado en SSLabs.

Para el caso de ETB, la evaluación de 2018 mejora en dos de los 4 ejes temáticos evaluados y mantiene el puntaje en los otros dos, en relación con el puntaje obtenido en el año anterior.



eTb	PUBLICIDAD	CLARIDAD	FACILIDAD	ACCESIBILIDAD	LENGUAJE INCLUSIVO (BONIFICACION)	SUMA POR CRITERIO	PROMEDIO POR EJE
COMPROMISOS POLÍTICOS							
Política de género	0,2	0,2	0,2	0,2		1	2
Política de accesibilidad						0	
Informes de transparencia	1	1	0,5	1		4	
INTIMIDAD							
Políticas de protección de datos	1	1	0,5	1		4	3
Informa la obligación legal de retención de datos	0,66	0,66	0,66	0,66		3	
Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	1	0,5	1		4	
Procedimiento de entrega de datos	1	1	0,5	1		4	
Notificación a las personas de entrega de datos						0	
LIBERTAD DE EXPRESIÓN							
Procedimientos de bloqueo	1	1	1	1		4	3
Procedimiento de cancelación	0,5	0,5	0,5	0,5		2	
Guía sobre comportamientos no permitidos	1	1	1	1		4	
SEGURIDAD DIGITAL							
Informa de fuga de datos personales y acciones de mitigación	0,33	0,33	0,33	0,33		1	3
Uso de protocolo de seguridad (HTTPS) en su sitio web	4					4	

COMPROMISOS POLÍTICOS

A pesar de contar con una "Política de Derechos Humanos", no se identifican los elementos que se califican en el criterio de política de género. Sin embargo, existe un documento titulado "Comité de Convivencia Laboral", en el que se incluye el compromiso de evitar y sancionar las conductas de acoso laboral. Este reconocimiento le merece parte del punto de la evaluación.

Por otro lado, no se encuentra una política de accesibilidad que pueda ser evaluada.

ETB fue reconocida en el informe de 2017 como la primera empresa en Colombia en publicar información que puede considerarse equivalente a la de los informes de transparencia internacionales. Para la fecha de esta evaluación, ETB mantuvo su compromiso actualizando los datos e información. También publica datos sobre la cantidad de peticiones que recibe, su procedibilidad y las entidades gubernamentales que hacen los requerimientos. La información de ETB está actualizada hasta el primer semestre de 2018.

INTIMIDAD

ETB cuenta con una "Política de Protección de Datos" que cumple con los requerimientos de la evaluación. Aunque es positivo que la política se encuentra en un sitio donde ETB recoge documentos de interés denominado "Transparencia y acceso a la información pública", el problema es que no es fácil llegar y encontrar estos documentos. Para encontrar el documento, se requieren 4 pasos y se llega desde la sección de "¿Quiénes Somos?" en la página principal. La práctica generalizada es ubicarlos en política de privacidad o similares. La mayoría de los documentos que se usaron en esta evaluación se encuentran en este sitio, por tanto, se afectan en la facilidad para su descubrimiento.

ETB informa en sus políticas que recoge y recopila datos personales, e informa el tiempo que los guarda. Ahora bien, su descripción es muy amplia. Indica que lo hace durante los plazos requeridos para llevar a cabo la gestión de sus diferentes áreas, pero no informa expresamente sobre sus obligaciones legales, aunque el informe de transparencia permite deducirlo.

En cuanto al criterio de informar las razones para responder a solicitudes de información de gobierno y personas privadas, su política de tratamiento de datos personales contempla unas "Reglas para poder compartir información personal con terceros", en donde se indica que, excepcionalmente, entrega información a las autoridades. También indica razones para compartir información con terceros.

ETB ha hecho un importante esfuerzo por describir su procedimiento de entrega de datos. Allí explica cómo atiende las solicitudes realizadas por el sector público, específicamente la Fiscalía y la Policía, para el tema de interceptación de comunicaciones, que

debe ser reconocido. Lo hace en varios documentos bajo el título de “intimidad” en la sección de “Transparencia y acceso a la información pública”. No hay documentos similares sobre la forma como entrega datos al Estado o personas privadas. En todo caso, en su informe de transparencia se deduce cuáles son las autoridades a las que entrega nuestros datos. El esfuerzo se reconoce con el punto en la calificación.

ETB no se compromete a notificar a las personas usuarias de sus servicios siempre que entrega sus datos a solicitud de un tercero.

LIBERTAD DE EXPRESIÓN

ETB publica el procedimiento para cumplir con las órdenes del Ministerio de las TIC de bloquear contenidos. Explica que se trata de una tarea diaria que, además, incluye verificar con las fuentes de la Policía.

Cuando abordamos la cancelación del servicio, se encuentran las “Políticas de Uso Aceptable”, donde se establecen las condiciones para usar los servicios de la empresa y las razones por las que se puede cancelar el servicio. Ahí, sin embargo, no se hace mención a procedimientos, por tanto, no es posible establecer si los mismos incluyen garantías para el debido proceso.

ETB cuenta con un código de conducta que establece las prohibiciones que tiene las personas usuarias de sus servicios y señala que los procedimientos de cancelación incluyen una segunda evaluación. Sin embargo, no hay una descripción de estos procedimientos.

SEGURIDAD DIGITAL

Si bien ETB cuenta con una política de seguridad de la información, esta no incluye los procedimientos para enfrentar brechas de seguridad. No indica cómo informan a las personas afectadas, a las autoridades ni hay una indicación del tipo de medidas que usan para mitigar daños.

ETB implementa correctamente el protocolo de seguridad HTTPS a lo largo de su portal web, que se verificado a través de un *Server Test* en SSLabs.

Para la evaluación de este año, DirecTV mejoró su calificación en uno de los tres ejes temáticos evaluados y se mantuvo en los otros tres, en comparación con los resultados obtenidos en el año anterior.

DIRECTV	PUBLICIDAD	CLARIDAD	FACILIDAD	ACCESIBILIDAD	LENGUAJE INCLUSIVO (BONIFICACIÓN)	SUMA POR CRITERIO	PROMEDIO POR EJE
COMPROMISOS POLÍTICOS							
Política de género	0,6	0,6	0,6	0,6		2	2
Política de accesibilidad						0	
Informes de transparencia	1	1	1	1		4	
INTIMIDAD							
Políticas de protección de datos	1	1	1	1		4	3
Informa la obligación legal de retención de datos	0,66	0,66	0,66	0,66		3	
Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	1	1	1		4	
Procedimiento de entrega de datos						0	
Notificación a las personas de entrega de datos	0,5	0,5	0,5	0,5		2	
LIBERTAD DE EXPRESIÓN							
Procedimientos de bloqueo						0	0
Procedimiento de cancelación						0	
Guía sobre comportamientos no permitidos						0	
SEGURIDAD DIGITAL							
Informa de fuga de datos personales y acciones de mitigación						0	2
Uso de protocolo de seguridad (HTTPS) en su sitio web	4					4	

COMPROMISOS POLÍTICOS

En primer lugar, sobre la política de género y los 5 elementos que se evalúan, se encontró un "Código de Ética y Conducta Empresarial" en el que se identificaron 3 de los 5 componentes: disposiciones sobre selección de personal, ascenso y capacitaciones, y prevención y sanción del acoso.

Dentro de los documentos públicos que se encuentran en el portal de Directv, no se encontró una política de accesibilidad ni tampoco herramientas que tuvieran como propósito facilitar el acceso de personas con discapacidad a la información contenida en su portal.

La matriz de Directv, AT&T, publicó un informe de transparencia en agosto 2018, donde se incluyen las solicitudes de bloqueo de IP. Directv mejoró su calificación este año porque el informe se publica ahora también en el sitio web de Directv Colombia y no solo en el de su matriz.

Si bien este informe mejora la información que comparte, insistimos –como lo hicimos en 2017– en que la información es insuficiente, porque no es clara en relación con el tipo de solicitudes que recibe por parte de terceros (sobre autoridades locales y cuáles o si provienen de privados) ni cómo, cuándo y porqué puede dar información de las personas que utilizan sus servicios. El propio informe es detallado sobre esto para EE.UU., pero la información de otros países que describe se refiere tan solo a solicitudes internacionales. Esto es insuficiente

Así, por ejemplo, de la información suministrada en este informe podemos establecer que después de las autoridades de México, las de Colombia son las que más solicitudes internacionales de información hacen a la multinacional, superando incluso a Venezuela, Brasil o Rusia. Sin embargo, no sabemos quién solicitó la información, qué información pidieron, etcétera, y no hay información y datos locales referidos al negocio de Directv en Colombia.

INTIMIDAD

Directv publica en su sitio una política de protección de datos y un aviso de privacidad que se descargan en documentos que tienen los requerimientos de la evaluación.

Su política describe el tipo de información que se recolecta y también indica el período por el que la conserva. Aunque no se refiere a plazos de retención legal, sí reconoce que los períodos de conservación de información son muy amplios. En su política, Directv da cuenta de las razones para responder a solicitudes de terceros que pidan nuestra información, por ejemplo, por una orden legal o un contrato comercial (con previo consentimiento de la persona titular).

Habría que mencionar que su política parece tener como punto de referencia algún país extranjero, pues habla de "ley federal". En el caso de Directv, el informe de transparencia no apoya dando más información para este criterio, en la medida en que la información no es sobre los requerimientos locales, sino los que se hacen a la matriz AT&T.

En 2018, tampoco se encuentra en el sitio web de Directv información relacionada con los procedimientos para entregar información a terceros ni por solicitudes legales a autoridades, ni a privados por motivos comerciales.

Finalmente, en relación con la notificación del uso de datos por terceros, Directv, en su política de privacidad, adquiere un compromiso con las personas que usan sus servicios al afirmar que cumple con requerimientos legales o judiciales de solicitud de información personal. Afirma que

> *en la mayoría de los casos en que la información se provee en respuesta a un requerimiento legal, nosotros le proveeremos notificación previa de dicho requerimiento u orden de modo que usted pueda impugnarla en un procedimiento en corte"*

Si bien no se puede decir que esta afirmación cumple con el requisito, pues es totalmente discrecional, es precisamente el sentido del compromiso que se busca lograr con este criterio. Por esta razón, se otorgó la mitad de la calificación como reconocimiento a este esfuerzo.

LIBERTAD DE EXPRESIÓN

Aunque Directv, como las demás empresas, tiene la obligación legal de evitar la propagación de material relacionado con el abuso y explotación sexual de niños, niñas y adolescentes, no publica en su sitio web documentos relacionados con los procedimientos que emplea para hacer el bloqueo de contenidos de este tipo o de cualquier otro.

La empresa tampoco tiene una guía de comportamientos no permitidos que facilite a quienes contratan sus servicios conocer cómo pueden perder o conservar su calidad de clientes.

Ahora bien, en el informe de transparencia de la matriz AT&T, que incluye la operación de Directv en Colombia, se informa de los bloqueos de IP o URL. No obstante, los datos que presentan no contribuyen con información local, sino que reflejan las solicitudes que se hacen a la matriz.

SEGURIDAD DIGITAL

En el "Manual pnterno de Políticas y procedimientos sobre tratamiento de datos personales de DirecTV Colombia LTDA", se encuentra un pequeño capítulo que ofrece apli-

caciones y procedimientos para mitigar el riesgo al que se pueden encontrar los datos de sus clientes. Dado que no especifica cuáles ni tampoco si notifica a las autoridades y a las personas que usan sus servicios, este elemento no se consideró en la evaluación.

A diferencia de lo que sucedía en 2017, se puede corroborar, según el Server Test de SSLabs, que Directv habilitó el protocolo de seguridad HTTPS en su sitio web. Ahora, el problema es que la mayoría de los documentos consultados para esta evaluación no contaban con esta protección, por tanto, la calificación se le disminuyó en este criterio pues da cuenta de una mala implementación.

En la evaluación de 2018, la calificación de Tigo-UNE mejoró respecto del puntaje de 2017. En dos de los cuatro ejes temáticos evaluados hubo mejor calificación, mientras que se mantuvo en otro y bajó en otro. Ahora bien, la razón de que bajara en uno de los ejes temáticos tiene que ver con que se hizo más estricta la evaluación, no con que la empresa deteriorara sus políticas.

tigo une	PUBLICIDAD	CLARIDAD	FACILIDAD	ACCESIBILIDAD	LENGUAJE INCLUSIVO (BONIFICACIÓN)	SUMA POR CRITERIO	PROMEDIO POR EJE
COMPROMISOS POLÍTICOS							
Política de género	0,4	0,4	0,2	0,4		1	2
Política de accesibilidad						0	
Informes de transparencia	1	1	1	1		4	
INTIMIDAD							
Políticas de protección de datos	1	1	1	1		4	3
Informa la obligación legal de retención de datos	0,66	0,66	0,66	0,66		3	
Informa las razones para responder a solicitudes de información de gobierno y personas privadas	1	1	1	1		4	
Procedimiento de entrega de datos	1	1	1	1		4	
Notificación a las personas de entrega de datos						0	
LIBERTAD DE EXPRESIÓN							
Procedimientos de bloqueo	0,5	0,5	0,5	0,5		2	2
Procedimiento de cancelación						0	
Guía sobre comportamientos no permitidos	1	1	1	1		4	
SEGURIDAD DIGITAL							
Informa de fuga de datos personales y acciones de mitigación	0,5	0,5	0,5	0,5		2	3
Uso de protocolo de seguridad (HTTPS) en su sitio web	4					4	

COMPROMISOS POLÍTICOS

Tigo-UNE publica un código de ética en el que habla de la necesidad de tener políticas inclusivas de diversidad sexual y de género. En este código se incluyen compromisos de la empresa en dos de los elementos evaluados: contratación y en temas de acoso, que incluye incentivos a la denuncia al interior de la empresa.

No se encontraron en su sitio web documentos de política de accesibilidad.

Para esta evaluación, se encontró que Tigo-UNE cuenta con dos documentos en donde publica información que en la evaluación se identifica como informe de transparencia.

En su informe de gestión de 2017 tiene un punto sobre páginas bloqueadas en donde explica el marco legal para la protección de niños y jóvenes que lo llevó a bloquear 11.946 páginas en 2017. También menciona que bloqueó 406 páginas en ese mismo período relacionadas con juegos de azar y por mandato del Decreto 4142 de 2011 de Coljuegos.

De otra parte, Tigo-UNE publicó recientemente un documento titulado "Requerimientos de datos personales por terceros y bloqueos de contenidos" que tiene información para 2017 y complementa lo que la empresa había publicado en su informe de gestión y sostenibilidad de ese mismo año, donde incluyó un aparte sobre páginas bloqueadas. El documento detalla los requerimientos recibidos y las autoridades que los hicieron tanto en móviles como en fijos. También describe el proceso interno para atender estos requerimientos y explica en forma sucinta el procedimiento que sigue para el bloqueo de páginas. No obstante, se enfoca en este caso en las relacionadas con material de abuso sexual infantil o alusivo a actividades sexuales de menores de edad.

INTIMIDAD

Tigo-UNE también creó un sitio diferente donde está centralizando la información que tiene sobre la forma como protege a las personas que usan sus servicios. En este sitio están las políticas de protección de datos de Tigo y de UNE (dos documentos diferentes) y el aviso de privacidad de la empresa que es unificado, además del documento sobre requerimientos de información ya mencionado. Adicionalmente, se encontró otro documento de políticas de privacidad para Tigo-UNE en el sitio de ayuda de la empresa. Si bien esto no es objeto de la evaluación, no parece una buena práctica tener tantos documentos de la misma temática.

En todo caso, los documentos cumplen formalmente con los criterios de evaluación.

Tigo-UNE no informa sobre su obligación de hacer retención de datos en el documento que es asimilable a un informe de transparencia. Se deduce esta obligación del marco legal que se ofrece y se indican el tipo de datos que suministra. En cuanto al plazo, Tigo-UNE cuenta con una disposición muy amplia de los términos durante los que guarda

los datos al señalar que las bases de datos permanecerán vigentes hasta que culmine la finalidad para la que fueron creadas. Agrega que los datos se mantendrán almacenados conforme a la autorización dada del tratamiento o si el titular la revoca, pero no se mencionan plazos de retención legal.

Tigo-UNE publica sus políticas de protección de datos en las que informa las razones por las que puede responder a solicitudes de información por parte del Gobierno o de otras entidades privadas y la complementa con la información del documento "Requerimientos de datos personales por terceros y bloqueos de contenidos", indicando que

> *en el año 2017 compartimos información, sin previa notificación, únicamente en los siguientes casos estipulados por la Ley: (i) requerimiento de una entidad pública o administrativa en ejercicio de sus funciones, (ii) orden judicial, (iii) entrega de datos de naturaleza pública o (iv) casos de urgencia médica o sanitaria.*

Allí mismo se puede establecer cuáles son las autoridades a las que responden solicitudes del sector público, incluida la Fiscalía. No hay detalles sobre el sector privado.

En relación con el procedimiento de entrega de datos, Tigo-UNE es la única de las empresas evaluadas que publica un flujograma en el que informa su procedimiento interno de respuesta para este tipo de requerimientos. El esfuerzo es reconocido con el punto completo en la calificación, aunque no se habla de los privados ni de sus procedimientos para interceptación de comunicaciones.

Tigo-UNE no cuenta con un compromiso de notificación a las personas usuarias de sus servicios siempre que entrega sus datos personales.

LIBERTAD DE EXPRESIÓN

En sus políticas de privacidad, incluyó su obligación legal para bloquear "material pornográfico o alusivo a actividades sexuales de menores de edad", indicando el marco legal que aplica. No hay una descripción del procedimiento que adelanta en este contexto, que permitiría verificar que se cumplen con garantías como la del debido proceso.

No se encontró ningún documento que permitiera evaluar el procedimiento de cancelación de cuentas que sigue la empresa.

En 2018, Tigo-UNE publicó un documento que da información sobre comportamientos no permitidos.

SEGURIDAD DIGITAL

Tigo-UNE tiene una política de seguridad digital que consiste sustancialmente en consejos preventivos y buenas prácticas. El documento incluye acciones de mitigación de riesgos, pero no aparece el compromiso de informar sobre brechas de seguridad que

puedan comprometer la información de las personas que contratan sus servicios ni a las autoridades ni a los afectados.

En relación con el protocolo de seguridad HTTPS, está habilitado en todo el portal web como fue corroborado a través del un Server Test en SSLabs.

La calificación de esta empresa mejora en dos de los cuatro ejes temáticos evaluados, pero empeora en otro, ya que en 2018 no se encontró el documento que le dio puntaje en el año anterior.

EMCALI	PUBLICIDAD	CLARIDAD	FACILIDAD	ACCESIBILIDAD	LENGUAJE INCLUSIVO (BONIFICACIÓN)	SUMA POR CRITERIO	PROMEDIO POR EJE
COMPROMISOS POLÍTICOS							
Política de género						0	1
Política de accesibilidad	1	1	1	1		4	
Informes de transparencia						0	
INTIMIDAD							
Políticas de protección de datos	1	1	0,5	1		4	1
Informa la obligación legal de retención de datos						0	
Informa las razones para responder a solicitudes de información de gobierno y personas privadas						0	
Procedimiento de entrega de datos						0	
Notificación a las personas de entrega de datos						0	
LIBERTAD DE EXPRESIÓN							
Procedimientos de bloqueo						0	0
Procedimiento de cancelación						0	
Guía sobre comportamientos no permitidos						0	
SEGURIDAD DIGITAL							
Informa de fuga de datos personales y acciones de mitigación						0	0
Uso de protocolo de seguridad (HTTPS) en su sitio web						0	

COMPROMISOS POLÍTICOS

No se encuentra documentos que permitan evaluar los componentes de este criterio en materia de género y de transparencia.

En cuanto a la política de accesibilidad, Emcali dispone de un *plugin* en el sitio web que permite mejorar la capacidad de las personas con discapacidad visual para conocer la información del sitio.

INTIMIDAD

Emcali, en la sección de transparencia, tiene su política de protección de datos y aviso de privacidad. Aunque los documentos están públicos, son claros y se pueden navegar y reutilizar, todavía hay espacio para que sea más fácil encontrarlos. La práctica es que estén anunciados en la página de inicio como protección al usuario o política de privacidad. Acá están como transparencia y toma 3 pasos llegar a ellos.

Ahora bien, el documento no ofrece detalles que permitan evaluar ninguno de los otros aspectos que se consideran en la metodología de ¿Dónde están mis datos? como elementos claves para proteger la intimidad.

LIBERTAD DE EXPRESIÓN

A pesar de encontrar en el aviso de privacidad del sitio de Emcali una mención a los bloqueos de páginas web, no se encuentran documentos que describan los procedimientos que sigue la empresa para esos bloqueos. Tampoco se encuentra información sobre la cancelación de servicios ni hay documentos que expliquen lo que esta empresa considera como comportamientos no permitidos.

SEGURIDAD DIGITAL

No se encuentra información para evaluar este criterio. En el sitio web tampoco se ha implementado el protocolo de transmisión segura HTTPS.

En 2018, la evaluación de Telebucaramanga mejora en un criterio de los cuatro evaluados, empeora en otro y no presenta cambios en otro, en comparación con el año anterior. La razón del deterioro en el puntaje tiene que ver con que se hizo más estricto, no con que se deteriorara el compromiso de la empresa.

telebucaramanga Somos de aquí	PUBLICIDAD	CLARIDAD	FACILIDAD	ACCESIBILIDAD	LENGUAJE INCLUSIVO (BONIFICACIÓN)	SUMA POR CRITERIO	PROMEDIO POR EJE
COMPROMISOS POLÍTICOS							
Política de género						0	1
Política de accesibilidad	1	1	1	1		4	
Informes de transparencia						0	
INTIMIDAD							
Políticas de protección de datos	1	1	1	1		4	2
Informa la obligación legal de retención de datos	0,66	0,66	0,66	0,66		3	
Informa las razones para responder a solicitudes de información de gobierno y personas privadas	0,5	0,5	0,5	0,5		2	
Procedimiento de entrega de datos						0	
Notificación a las personas de entrega de datos						0	
LIBERTAD DE EXPRESIÓN							
Procedimientos de bloqueo						0	0
Procedimiento de cancelación						0	
Guía sobre comportamientos no permitidos						0	
SEGURIDAD DIGITAL							
Informa de fuga de datos personales y acciones de mitigación						0	2
Uso de protocolo de seguridad (HTTPS) en su sitio web	4					4	

COMPROMISOS POLÍTICOS

En 2018 no se encontró en el sitio de Telebucaramanga políticas de género.

En relación con la accesibilidad, se encuentra un aplicativo en el portal web con el que personas con discapacidad pueden hacer uso del mismo. Aunque no es una política, se le otorga el puntaje porque al final lo que se consigue es que las personas con discapacidad, efectivamente, puedan ejercer su derecho a informarse sobre los servicios de la empresa.

En relación con los documentos que pudieran significar que hay información equivalente a la que se publica en el informe de transparencia, tampoco se encontraron estos datos.

INTIMIDAD

Telebucaramanga cuenta con una política de protección y tratamiento de datos y un aviso de privacidad que se descarga de la sección de "Protección al usuario y normativa". Los documentos que se encuentran cumplen con los requerimientos de la evaluación.

La política que publica Telebucaramanga expone su obligación legal de recopilar datos así como el tipo de datos recolectados, pero no indica el tiempo de conservación.

En relación con las razones por las cuales comparten información con terceros, el documento señala en su acápite "Tratamiento y Finalidad" que puede compartir información con terceros privados para verificar información del comportamiento comercial, control y fraude o actividades con fines publicitarios. No aparece información relacionada con el sector público.

No se encuentra un documento que describa el procedimiento para entregarle información a terceros, como lo hacen otras empresas. Telebucaramanga afirma su deber de informar al titular sobre el uso de sus datos cuando este haga solicitud de ello. Esta afirmación no da puntos en la evaluación, porque no es un compromiso de informar siempre que entreguen los datos personales de alguien que usa sus servicios a un tercero.

LIBERTAD DE EXPRESIÓN

No se encuentran documentos relacionados con los procedimientos que se analizan en este aparte sobre bloqueo, cancelación o la guía de comportamientos no permitidos.

SEGURIDAD DIGITAL

En el documento "Políticas de seguridad en la red y prevención de fraudes", la empresa expone una serie de medidas para mitigar los riesgos de seguridad. Sin embargo, ninguno de estos documentos describe su compromiso para notificar a las autoridades y a las personas usuarias cuando se presente una brecha de seguridad, ni listan el tipo de acciones que usan para mitigar los riesgos.

Finalmente, el test de SSLabs indica que en el sitio web se implementa correctamente el protocolo de seguridad HTTPS.

METODOLOGÍA

I. EJES TEMÁTICOS

Para la realización de ¿Dónde están mis datos? 2018 seguimos trabajando en un sistema de evaluación basado en la necesidad de examinar los compromisos públicos de las empresas proveedoras de internet tanto en el aspecto de políticas corporativas, como en el respeto y la atención que ofrecen a la intimidad, la libertad de expresión y la seguridad digital de las personas que usan sus servicios.

En consecuencia, los ejes que evaluamos son:

Compromisos políticos. Entendemos por políticas el "Conjunto de conceptos, decisiones, programas y acciones con sentido deliberado y específico cuyo avance y proceso debe examinarse en forma permanente".[14] Es decir, las políticas que las empresas adoptan en diferentes temas es la forma como materializan sus compromisos políticos. Son la manera en la que las empresas dan importancia a problemáticas sociales. Nos interesa analizar y promover aquellas con las que estas empresas pueden generar un compromiso hacia la inclusión e igualdad, y una responsabilidad frente a la transparencia de sus operaciones. Inicialmente, la manera en la que medimos esto es considerando que las empresas tengan políticas de género y de accesibilidad para personas con discapacidad, y que publiquen un informe de transparencia (o su equivalente) para Colombia, al menos anualmente.

Intimidad. A través de formas concretas, las empresas demuestran el respeto a la intimidad de las personas que contratan sus servicios. La intimidad es un derecho fundamental reconocido en el Artículo 15 de la *Constitución Política de Colombia*. La evaluación busca ir más allá de las normas de protección de datos, por lo que se evalúa que las empresas adopten políticas de protección de datos. Además, se tiene en cuenta que informen sobre la obligación legal que tienen de retener datos, las bases legales por las que están obligadas a atender solicitudes de información de datos personales, los procedimientos que usan para entregar esos datos y si notifican a las personas sobre la entrega de su datos a terceros.

14 Atehortúa, A. y Rojas, D.. (2009). Cifras, impacto y perspectivas de la política de consolidación de la seguridad democrática. Balance 2006-2009. *Reflexión para la planeación*. Colombia: Ediciones Aurora.

Libertad de expresión. El rol de las empresas proveedoras de internet es clave para el respeto a la libertad de expresión de las personas que contratan sus servicios. Considerando que la libertad de expresión es un derecho fundamental reconocido en el Artículo 20 de la *Constitución Política de Colombia*, en nuestra evaluación tenemos en cuenta que las empresas realicen un esfuerzo por proteger ese derecho a través de la divulgación de sus procedimientos de bloqueo y de la cancelación de servicios. Además, consideramos que la empresa tenga una guía de comportamientos no permitidos que le posibilite a las personas entender cuáles son sus derechos y sus deberes en ese sentido.

Seguridad digital. Las empresas demuestran a través de acciones concretas su compromiso de garantizar la seguridad de sus productos y servicios. Nuestro interés en que la seguridad digital haga parte de la agenda de las empresas, en aras de la protección de la información privada de las personas que acceden a sus servicios de internet, es prioritario. Por ello, en nuestra evaluación del 2018 también tuvimos en cuenta dos acciones concretas de las empresas. Por un lado, analizamos si informan sobre los procedimientos que emplean en caso de sufrir brechas de seguridad y, por otro, evaluamos si utilizan el protocolo seguro de transmisión de datos (HTTPS) en todos sus sitios web y, particularmente, en aquellos en los que existe un intercambio de información (compras, ventas y/o consultas).

II. CRITERIOS DE EVALUACIÓN

Son los criterios que evaluamos en cada uno de los ejes.

DEFINICIÓN DE CRITERIOS	
1. Compromisos políticos	
1.1. Política de género	La empresa publica en su sitio web para Colombia una política comprometida con la promoción de la igualdad de género que, idealmente, incluye acciones concretas en las siguientes áreas: (1) selección y contratación de personal (diversidad sexual y de género); (2) desarrollo de carreras incluyendo capacitación y ascensos a puestos directivos; (3) equilibrio familiar-laboral (e igualdad en beneficios); (4) prevención del acoso sexual; y (5) promoción de imágenes públicas no sexistas.
1.2. Política de accesibilidad	La empresa publica en el sitio web para Colombia una política que promueva el mismo acceso y uso de los recursos electrónicos (ej. sitio web) y de información de sus servicios para personas con discapacidad.

Continúa tabla...

DEFINICIÓN DE CRITERIOS	
1.3. Informes de transparencia	La empresa publica periódicamente en su sitio web para Colombia un conjunto de documentos que aborden la forma en que (1) responden a solicitudes de datos personales por parte de terceros (ej. sector público); (2) ofrezcan claridades sobre la forma en que gestionan esos procesos; (3) si hacen o no noticaciones pertinentes y puntuales a las personas titulares de los datos; y (4) que incluye una explicación de su rol y de los criterios que emplean en los bloqueos y/o retiros de contenidos, cancelaciones o suspensión de servicios.
2. Intimidad	
2.1. Políticas de protección de datos	La empresa publica en el sitio web para Colombia su política de protección de datos.
2.2. Informa la obligación legal de retención de datos	La empresa informa públicamente que está obligada por ley a retener datos, el tipo de datos que retiene y el tiempo por el que los retiene.
2.3. Informa las razones para responder a solicitudes de información del sector público y personas privadas	La empresa da a conocer las bases legales o contractuales, las razones por las que está obligada o ha acordado cumplir con solicitudes de datos personales por parte del sector público y/o personas privadas. Esto incluye informar sobre la posibilidad de dar acceso a la Fiscalía al tráfico de las comunicaciones que cursen por las redes de la empresa o a dar acceso a datos personales a terceros privados como parte de acuerdos comerciales (ej. publicidad).
2.4. Procedimiento de entrega de datos al sector público y a privados	La empresa da a conocer su procedimiento para responder a solicitudes de información del sector público o de personas privadas. Para ello, por ejemplo, ofrece una guía de los criterios o protocolos que sigue para atender a estas solicitudes.
2.5. Notificación a las personas sobre la entrega de datos a terceros	La empresa notifica a las personas titulares de datos siempre que entrega su información en cumplimiento de un requerimiento de solicitud por parte de un tercero.
3. Libertad de expresión	
3.1. Procedimientos de bloqueo	La empresa publica en el sitio web para Colombia (1) los procedimientos que emplea para filtrar, retirar o bloquear contenidos indicando los soportes legales (ej. pornografía infantil) y/o (2) las obligaciones contractuales que lo justifican. Aplica en estos procedimientos el debido proceso y, como mínimo, tiene un procedimiento para atender quejas de cualquier persona que crea haber sido indebidamente bloqueada. Estos procedimientos cuentan con criterios de proporcionalidad y necesidad.

Continúa tabla...

DEFINICIÓN DE CRITERIOS	
3.2. Procedimiento de cancelación	La empresa publica en la sitio web para Colombia los procedimientos que emplea para suspender y/o cancelar servicios. El debido proceso y, como mínimo, se envía notificación a la persona afectada para que tenga la oportunidad de defenderse se aplican en estos procedimientos. Estos procedimientos, además, cuentan con criterios de proporcionalidad y necesidad.
3.3. Guía sobre comportamientos no permitidos	La empresa publica en el sitio web para Colombia un código de conducta para guiar a las personas en los comportamientos no permitidos en sus redes y servicios con el fin de evitar sanciones.
4. Seguridad digital	
4.1. Informa los procedimientos para cumplir la obligación legal de informar brechas de seguridad	La empresa informa públicamente su procedimiento para responder a las brechas de seguridad, incluyendo (1) notificación sin demora indebida a las autoridades pertinentes; (2) notificación a las personas afectadas, y (3) el tipo de medidas que la empresa puede tomar para mitigar los daños.
4.2. Uso de protocolo mejorado de transmisión de datos (HTTPS) en su sitio web	La empresa tiene activado de forma predeterminada el protocolo seguro de transmisión de datos (HTTPS) en el sitio web de Colombia.

III. INDICADORES DE EVALUACIÓN

A. INDICADORES PARA LA EVALUACIÓN DE CRITERIOS BASADOS EN DOCUMENTOS

En este examen, empleamos un sistema de indicadores que nos permite medir la forma como las empresas proveedoras actúan frente a cada uno de los criterios evaluados:

1. ***Publicidad***. Que la información esté publicada. Entendemos que la información es pública cuando se encuentra en el sitio web de la empresa en Colombia y está disponible en español.

   La valoración se hace de la siguiente manera:

   - El documento es público en el sitio web de la empresa en Colombia y está disponible en español. (1 punto)

- El documento es público pero no aparece en el sitio web de la empresa en Colombia y/o está en otro idioma. (0,5 puntos)
- El documento no se encuentra disponible en el sitio web de la empresa en Colombia ni está disponible en español. (0 puntos)

2. ***Claridad.*** Que la información sea presentada en un lenguaje no técnico, comprensible para cualquier persona. Esto quiere decir que la información es comprensible para un público amplio, no especializado, de diferentes edades y en contextos sociales y culturales diversos.

   La valoración se hace computando los resultados de la evaluación realizada por Fundación Karisma y por dos personas externas. Las personas externas representan perfiles no especializados (ni en tecnología ni en derecho) y divergen tanto en género como en edad. Cada una examina partes aleatorias de los textos publicados por las empresas en relación con los criterios de evaluación de ***¿Dónde están mis datos?***

   Para evaluar la claridad, Fundación Karisma y las personas externas deben leer los textos y escoger la afirmación que mejor represente cada texto de la siguiente manera:

   - El texto está escrito en forma sencilla, es de fácil comprensión, no tiene lenguaje técnico o, teniendo lenguaje técnico, está suficientemente explicado y no genera confusiones. (1 punto)
   - El texto está escrito de forma moderadamente compleja, contiene lenguaje técnico que no es suficientemente claro o no está adecuadamente explicado, lo que dificulta su comprensión. (0,5 puntos)
   - El texto está escrito en forma muy compleja, contiene mucho lenguaje técnico que no está explicado y no se logra su comprensión. (0 puntos)

3. ***Facilidad.*** Que la información sea fácil de encontrar en el sitio web de la empresa en Colombia (número de clics). Entendemos que la información es fácil de encontrar cuando se encuentra en el sitio web principal de la empresa y/o tiene un enlace que lleva directamente a esta.

   La valoración se hace de la siguiente manera:

   - 1 a 2 clics = muy fácil (1 punto)
   - 3 a 4 clics = fácil (0,5 puntos)
   - 5 o más clics = difícil (0 puntos)

4. ***Accesibilidad.*** Que el mayor número de personas, incluidas aquellas que tienen algún tipo de discapacidad o dificultad para la lectura, puedan utilizar y acceder a la información.

En la evaluación de este año solamente tuvimos en cuenta que la información esté presentada en un documento navegable, en el que puedan realizarse búsquedas y del que se puedan copiar y pegar partes. Entendemos que esto último aumenta la posibilidad de que la información sea usada efectivamente por más personas para indagar sobre sus derechos y deberes. Además, mejora la probabilidad de que los lectores automáticos la reconozcan para beneficio de personas con dificultad para la lectura.

La valoración se hace de la siguiente manera:

- El documento es navegable, permite búsquedas y se pueden copiar partes del texto. (1 punto)
- El documento es navegable o permite búsquedas o se pueden copiar partes del texto. (0,5 puntos)
- El documento no es navegable, no permite búsquedas ni copiar partes del texto. (0 puntos)

5. ***Lenguaje inclusivo.*** Este año, nuevamente, no dimos un puntaje al lenguaje inclusivo dentro de la evaluación. Los esfuerzos que las empresas hagan por hacer más incluyentes sus documentos fueron tenidos en cuenta y se bonificaron hasta con un (1) punto. Respecto al lenguaje inclusivo y su importancia en una política de género y contra la discriminación se puede consultar:
   - *Guía para el lenguaje incluyente* de la Alcaldía Mayor de Bogotá, Colombia.[15]
   - *Manuales y textos para el lenguaje incluyente*, recopilados por la Universidad Nacional de Colombia.16
   - *Guía para el lenguaje inclusivo y no discriminatorio* de CETEO en España.[17]
   - *Guía para la revisión del lenguaje desde una perspectiva de género*, elaborado por la Dra. Mercedes Bengoechea de la Universidad de Alcalá de Henares, España.[18]

15 Alcaldía Mayor de Bogotá. (2015). *Guía para el lenguaje incluyente*. Bogotá, Colombia: Secretaria Distrital de Hacienda. Disponible en http://www.shd.gov.co/shd/sites/default/files/documentos/todo_guia_lenguaje.pdf.

16 Universidad Nacional de Colombia. (s.f.) *Manuales y textos sobre lenguaje incluyente*. Disponible en http://www.humanas.unal.edu.co/nuevo/titulo-manuales-y-textos-sobre-lenguaje-incluyente/

17 CETEO. (s.f.) *Guía para el lenguaje inclusivo y no discriminatorio*. Disponible en http://www.aspaymcyl.org/pdf/Memorias/GUIA%20LENGUAJE%20NO%20SEXISTA%20E%20INCLUISVO_CETEO.pdf.

18 Bengoechea, M. (s.f.). *Guía para la revisión del lenguaje desde una perspectiva de género*. Disponible en http://www.bizkaia.eus/home2/Archivos/DPTO1/Noticias/Pdf/Lenguaje%20Gu%C3%ADa%20lenguaje%20no%20sexista%20castellano.pdf.

B. INDICADOR PARA EL CRITERIO TÉCNICO DE SEGURIDAD DIGITAL: IMPLEMENTACIÓN DEL PROTOCOLO HTTP

Implementar el protocolo HTTPS es la mínima medida de seguridad digital que deben aplicar los responsables de sitios web. Es una práctica que cada vez más se exige a los administradores de sitios web con el fin de proteger las información de las personas. Sin embargo, en algunos casos, aunque se tiene una versión segura del sitio, se ofrece acceso a una versión insegura de forma predeterminada. Esta es una mala práctica.

Para que se otorguen cuatro puntos en la evaluación de este criterio, se requiere que la empresa tenga implementado de forma predeterminada el protocolo HTTPS en la totalidad de su sitio web. Es decir, que cuando una persona escribe en su navegador la dirección web de la empresa entra automáticamente a la versión segura del sitio.

Es posible que, en algunas circunstancias, las personas entren a la versión segura del sitio web a pesar de que la empresa no tienen activada de forma predeterminada la implementación del protocolo HTTPS:

- Ingresando al sitio web de la empresa a través de buscadores que redireccionan a la versión segura del mismo. En esos casos, el mérito es del buscador, no de la empresa.
- Instalando complementos a los navegadores (ej. HTTPS Everywhere) que despliegan de forma automática la versión segura de los sitios web, a pesar de que no sea la versión predeterminada. Nuevamente, en este caso, el mérito no es de la empresa, sino de la persona.
- Implementación parcial del protocolo HTTPS para algunas páginas del sitio web (ej. páginas donde hay intercambio de información como compras o autenticaciones).

En ninguno de estos casos otorgamos puntaje por no cumplir con los componentes del criterio: implementación del protocolo HTTPS y uso en forma predeterminada. En suma, si no se tiene HTTPS predeterminado en el sitio no se obtiene puntaje. Ahora bien, excepcionalmente se reconocerá la mitad del puntaje si a pesar de que se encuentra HTTPS implementado por defecto, por situaciones anómalas se encuentra que no es realmente así, como cuando los documentos que se usan en la evaluación no están dentro de esta implementación.

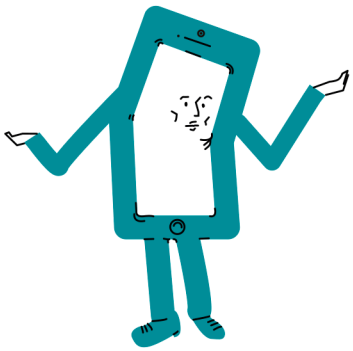
El informe ¿Dónde están mis datos? 2018 es la cuarta publicación que realiza la Fundación Karisma de esta serie.

Esta investigación busca impulsar que las empresas proveedoras de internet ofrezcan más información a quienes usan sus servicios y mejorar así nuestra capacidad para hacer efectivos nuestros derechos.

Para conocer y descargar el texto completo de este año visita https://karisma.org.co/donde-estan-mis-datos-2018/.

Para descargar el informe ejecutivo visite https://karisma.org.co/descargar/informe-ejecutivo-donde-estan-mis-datos-2018/

Puedes conocer los informes anteriores en https://karisma.org.co/DEMD/



INFORME **2018**

¿DÓNDE ESTÁN MIS DATOS?

INVESTIGADORA: CAROLINA BOTERO

ASISTENTE DE INVESTIGACIÓN: DAVID MARTÍN ESPITIA

karisma.org.co

Twitter: **@Karisma**

Facebook: **@fundacionkarismaa**

Con el apoyo de:

ELECTRONIC FRONTIER FOUNDATION

accessnow